

Hardware: Compaq Proliant DL380 G4
4GB of Memory
Intel Xeon CPU 3.80GHz

Operating System: Microsoft Windows Server 2003 R2 Enterprise Edition

Service Pack: SP2

Server Name: SWASHMN0742E

DOMAIN: web.ams.usda.gov

Hard Disk Drives: C: 68GB (Local Disk) E: 11GB (Utilities) F: 40GB (MNCS Data)

BackWeb Version: 6.1.2

The Market News Communication System (MNCS) is a collection of components, both Commercial Off-The Shelf (COTS) and custom coded, which deliver updated market information to the end user.

Windows Users and Groups

For the Market News Communication System to work properly, the BackWeb server needs to be configured with a specific account. A local user called “mncs_nt1” needs to be created. This user should be a member of the “Administrators” group, and must have the same account name and password as the “mncs_nt1” account in the “AMSMARKET_NEWS” domain.

Files and Shares

The second RAID Logical Unit (formatted as the F: partition under Windows Server 2003) is used to store the mkt_news directories. The following configuration should be used for these directories:

- The partition used for the F: drive should be formatted with NTFS
- The NTFS Permissions on the root of the F: drive should be assigned as follows:
 - Administrators: Full Control
 - SYSTEM: Full Control
- The **mkt_news** and **mkt_news2** directories should be created in the root of the F: drive
- The **mkt_news** and **mkt_news2** directories should be shared (with the same names).
- The share permissions for both directories should be:
 - Administrators: Full Control
 - SYSTEM: Full Control

The following are components and their interaction:

- **The “MNCS” application.** This is a custom designed application (written in Visual Basic) which is utilized by USDA employees to submit reports to the system.
- **The “SERVERX” process.** This is a custom designed application (written in C) which runs on the AMSMN1 server. It is responsible for disseminating content to various locations/servers. It is sometimes referred to as the “Traffic Cop” of the MNCS system.

- **BackWeb Client-Server Application.** This is a COTS application which is utilized to distribute new content to the end user as soon as it is available. The Server component runs on BackWeb servers maintained by Market News and the client component runs on workstations of the end user.
- **Site Server Content Replication Service.** This is a COTS application for replicating Web content to multiple locations. Within the Market News system, it is utilized to move content from the Staging Server to the live web servers.
- **Archive Batch process.** This is a custom designed batch file which archives Market News reports and is run on a daily basis.
- **USDA Client.** This is a custom designed application which runs on the end user desktop. It is designed to work in conjunction with the BackWeb Client software to extract the desired reports from downloaded content.

REPORT GENERATION AND DISTRIBUTION

USDA employees generate the various Market News reports on their desktops. These systems may be located internally (on the backbone), or at a remote location (accessible via dial-up). Once the reports have been generated, they are submitted either through the “MNCS” application (a custom developed Visual Basic program), or by manually copying the resulting text file to the AMSMN1 computer (**Figure 1**).

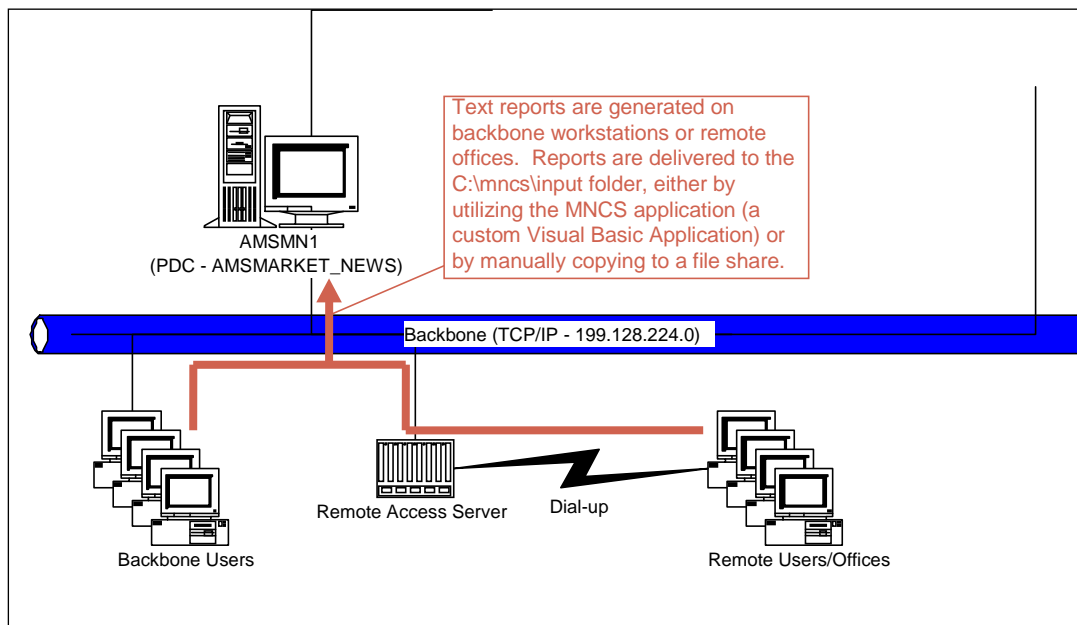


Figure 1: Market News Report Generation

On the AMSMN1 Server, the SERVERX.EXE application periodically monitors the “Input” folder. When a new report is detected, the SERVERX application is responsible for disseminating the report to a number of locations, including the Staging Server (AMS-LIVE web site), and the Backweb Servers (**Figure 2**).

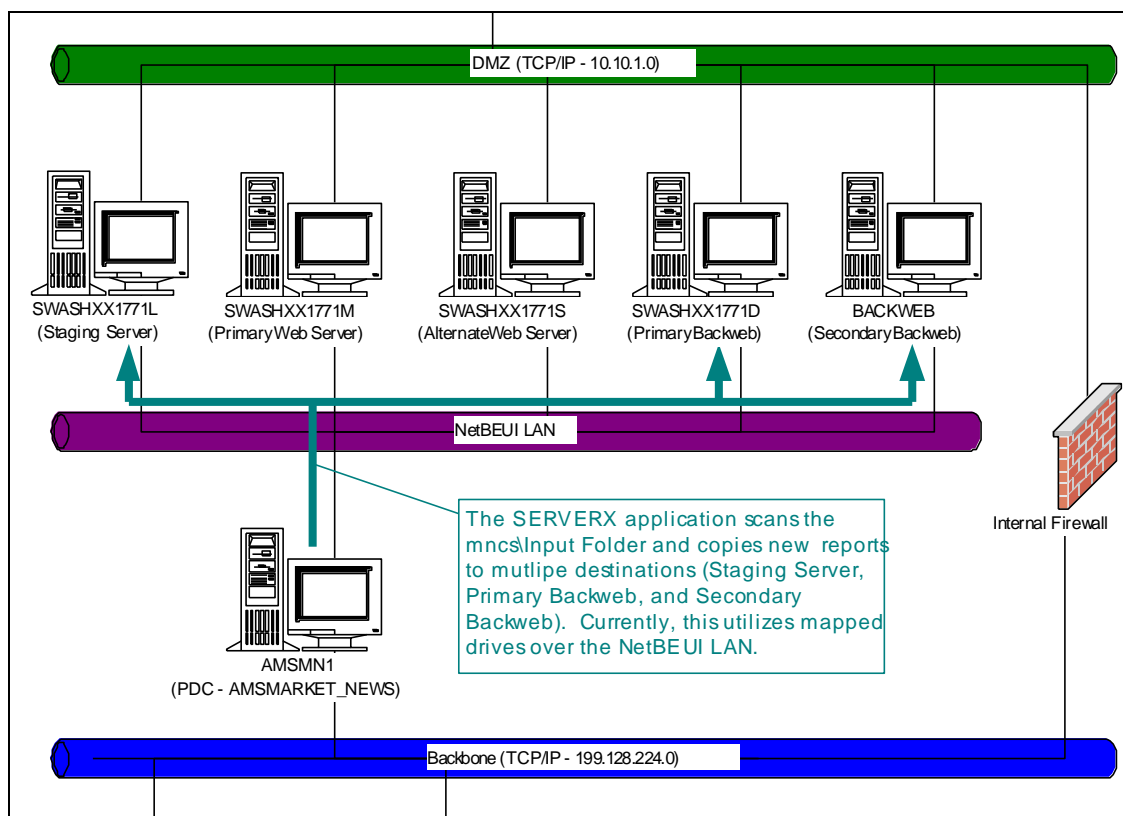


Figure 2: SERVERX.EXE Dissemination

The SERVERX application requires that certain drive mappings are present to copy the files to the destination servers, as summarized in **Table 1**:

AMSMN1 Drive Letter	Mapped To
H:	\\SWASHXX1771L\mncs (this is used by the Archive Batch process)
L:	\\SWASHXX1771L\Day1
M:	\\SWASHXX1771L\Web-BBS
P:	\\SWASHXX1771D\mkt_news
Q:	\\SWASHXX1771D\mkt_news2
U:	\\BACKWEB\mkt_news
V:	\\BACKWEB\mk_news2
W:	\\BACKWEB\InetPub (no longer in use)

Table 1: Current Drive Mappings for SERVERX Application

These drive mappings currently traverse the NetBEUI LAN segment. Name resolution is achieved by broadcasting on the NetBEUI segment. Prior to the installation of the Internal Firewall, this was the only mechanism for the AMSMN1 server to connect to the target servers on the DMZ.

The SERVERX application is run under the security context of the mncs_nt1 account, on the AMSMARKET_NEWS domain. Share and NTFS permissions on the destination servers are configured to give the mncs_nt1 account the access that it requires to write the data to the destination folders.

On the Staging Server (SWASHXX1771L), Site Server Content Replication Service (CRS) monitors various directories (including those with market news reports) for any change in content. When the SERVERX process copies new files to the staging server, CRS immediately replicates those files to the Primary and Secondary web servers (SWASHXX1771M and SWASHXX1771S) and the off-site backup in Fresno (on a scheduled basis), as shown in **Figure 3**.

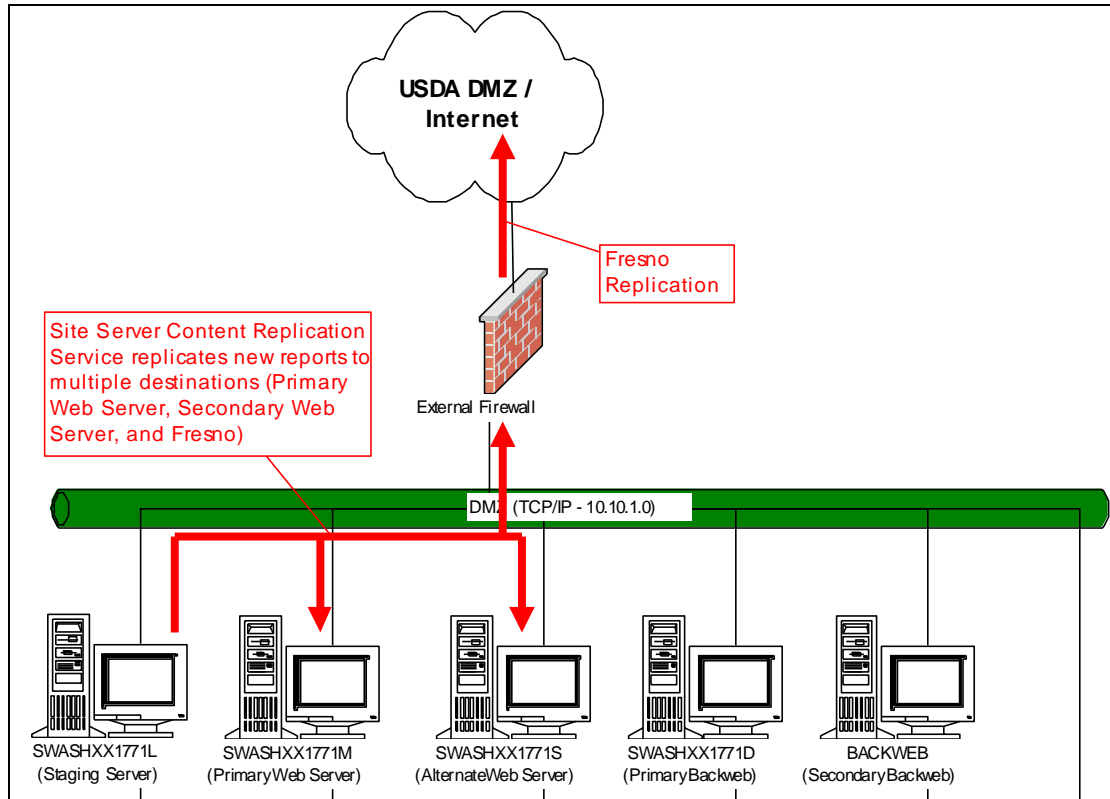


Figure 3: Site Server Content Replication Service

CLIENT RETRIEVAL

There are two mechanisms through which clients can retrieve market news reports, the AMS web site and the Backweb Client/Server application.

AMS Web Site

Once the Content Replication Service has replicated the report files to the web servers, that content is immediately available for download through the AMS web site. End users connect to the AMS web site through any browser and manually request specific reports (**Figure 4**).

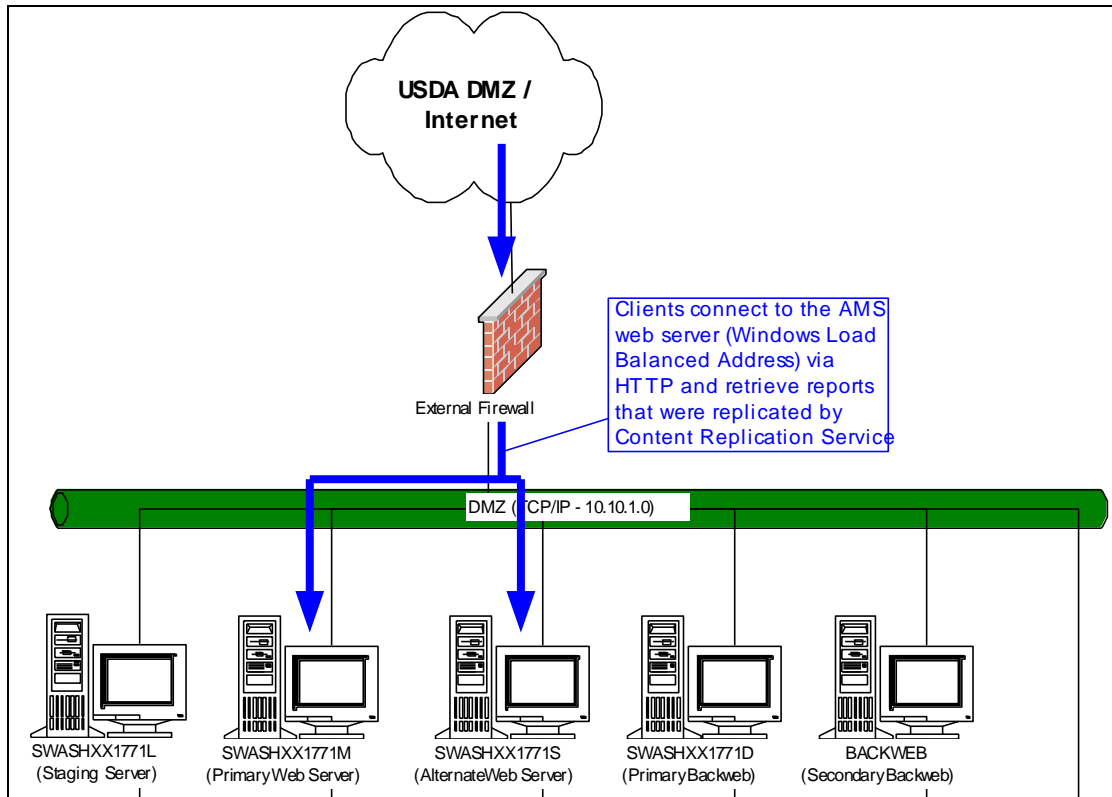


Figure 4: Web Clients

Backweb Client/Server Application

The Backweb Client/Server application allows updated content to be automatically distributed to the end user. When new reports are copied to the Backweb server, a custom PERL application running on the Backweb server (USDA1.pl) detects this data and packages it in a format compatible with the Backweb delivery mechanism (the INFOPAK format).

The Backweb Client software polls the Backweb server on a regular basis, checking for new INFOPAKs. When updated INFOPAKs are available, they are downloaded to the client's machine, (**Figure 5**).

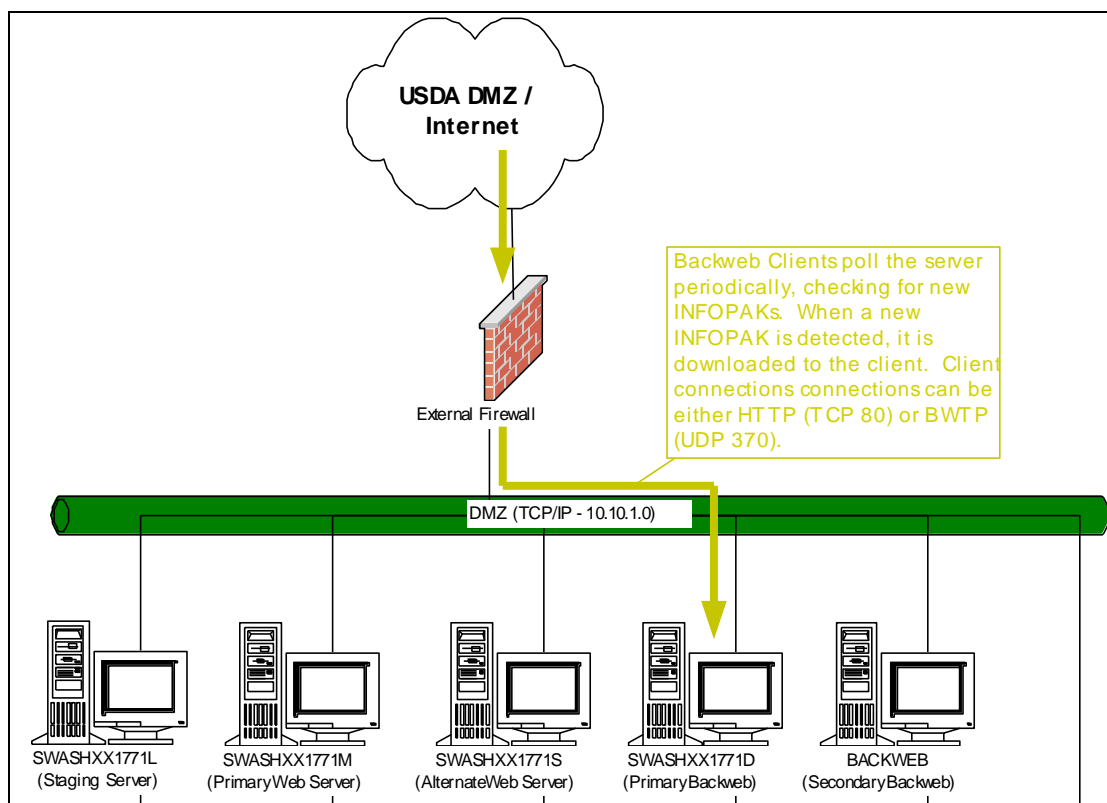


Figure 5: Backweb Clients

There are two protocols which can be utilized for Backweb Client/Server connectivity. The protocol used is determined by the configuration of the client software. By default, HTTP is utilized (TCP port 80). The Backweb client software can also be configured to utilize the Backweb Transfer Protocol (BWTP), which utilizes UDP port 370. HTTP appears to provide a quicker response and faster downloads, but also utilizes more of the client's bandwidth. The server will answer requests sent with either protocol.

On the client's workstation, the "USDA Client" (developed specifically for Market News), extracts the plain text reports from the downloaded INFOPAKs, compares them to the list of desired reports (configured by the end user), and delivers the desired report files to a directory on the client machine (C:\USDA by default).

Archive Process

The Archive Batch process runs on the AMSMN1 server on a daily basis. (Currently, it is scheduled to run at 4:00 AM every morning). This batch file performs two primary functions:

1. The previous day's reports (located in the Staging Server's "Day1" directory) are copied to the archive. (The path for the archive destination is edited manually on a daily basis)
2. Once the files have been copied, they are deleted from the "Day1" directory to make room for the current day's reports.

AUTHENTICATION

There are three Windows NT 4.0 Domains involved with the Market News system: AMSMASTER, AMSMARKET_NEWS, and AMS_INTERNET. One-way trust relationships have been established between the domains, as shown in **Figure 6**.

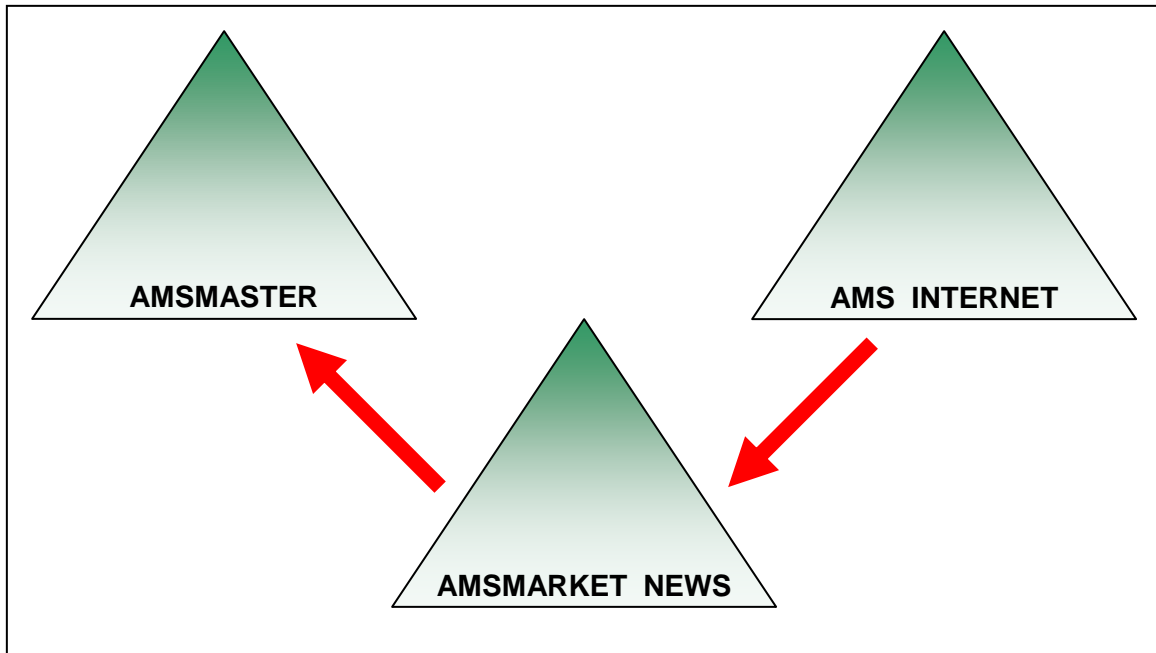


Figure 6: Trust Relationships

The AMS_INTERNET domain trusts the AMSMARKET_NEWS domain, which trusts the AMSMASTER domain. This allows machines in the AMS_INTERNET domain to assign permissions to users or groups in the AMSMARKET_NEWS domain. This is reflected in the NTFS and share permissions assigned to the shares which AMSMN1 connects to. **Table 2** lists those permissions as they are currently configured (Note that “MNCSAdminGlo” is a global group in the AMSMARKET_NEWS domain which contains the mncs_nt1 account):

The SERVERX application requires that a user is logged on to the AMSMN1 server at all times. The mncs_nt1 account is used for this. All the network connections utilized by the SERVERX applications are made under this security context.

Server	Path	Share Permissions	NTFS Permissions
SWASHXX1771L	E:\mncs	AMS_INTERNET\Domain Admins: Full AMSMARKET_NEWS\MNCSAdminGlo: Full Everyone: Read	AMS_INTERNET\Domain Admins: Full SWASHXX1771L\SYSTEM: Full AMSMARKET_NEWS\MNCSAdminGlo: Full SWASHXX1771L\IUSR_SWASHXX1771L1: Read Everyone: Read
SWASHXX1771L	E:\mncs\archive\day1	AMS_INTERNET\Domain Admins: Full AMSMARKET_NEWS\MNCSAdminGlo: Full Everyone: Read	AMS_INTERNET\Domain Admins: Full SWASHXX1771L\SYSTEM: Full AMSMARKET_NEWS\MNCSAdminGlo: Full SWASHXX1771L\IUSR_SWASHXX1771L1: Read Everyone: Read
SWASHXX1771L	E:\Web-BBS	AMS_INTERNET\Domain Admins: Full AMS_INTERNET\ArcanaSecurity: Full AMS_INTERNET\gdemery AMSMARKET_NEWS\MNCSAdminGlo: Full Everyone: Read	AMS_INTERNET\Domain Admins: Full AMSMARKET_NEWS\MNCSAdminGlo: Full SWASHXX1771L\SYSTEM: Full SWASHXX1771L\IUSR_SWASHXX1771L1: Read Everyone: Read
SWASHST1757D	C:\mkt_news	Everyone: Full	SWASHST1757D\Administrators: Full SWASHST1757D\Creator/Owner: Full SWASHST1757D\SYSTEM: Full Everyone: Change
SWASHST1757D	C:\mkt_news2	Everyone: Full	SWASHST1757D\Administrators: Full SWASHST1757D\Creator/Owner: Full SWASHST1757D\SYSTEM: Full Everyone: Change
BACKWEB	C:\mkt_news	Everyone: Full	BACKWEB\Administrators: Full BACKWEB\Creator/Owner: Full BACKWEB\SYSTEM: Full

			Everyone: Change
BACKWEB	C:\mkt_news2	Everyone: Full	BACKWEB\Administrators: Full BACKWEB\Creator/Owner: Full BACKWEB\SYSTEM: Full Everyone: Change
BACKWEB	C:\InetPub	AMSMARKET_NEWS\mnsc_nt1: Full	BACKWEB\Administrators: Full BACKWEB\Creator/Owner: Full BACKWEB\SYSTEM: Full AMSMARKET_NEWS\mnsc_nt1: Full

Table 2: NTFS and Share Permissions

REQUIRED CHANGES AND THEIR IMPACT

As a part of the AMS DMZ architecture redesign, there are some changes which will affect the configuration of the Market News system (primarily the distribution of files from the AMSMN1 server to the DMZ servers via the SERVERX application). The following sections describe those changes, the impact they will have on the Market News system, and the steps which will be required to ensure continuity of operations.

REMOVAL OF THE AMS_INTERNET DOMAIN

During the course of the DMZ architecture changes, the AMS_INTERNET domain will be phased out. All the DMZ servers that are currently members of this domain will become stand-alone servers. This will have repercussions with regard to the Market News, as the mapped drives which the SERVERX process utilizes are connected using authentication provided by the trust relationship between the AMSMARKET_NEWS and AMS_INTERNET.

Moving to a stand-alone mode for the destination servers will require that an alternate method of authentication is available. This will be in the form of synchronized local accounts, specifically that a local account on each destination server will be created with the same account name and password as exists on the AMSMARKET_NEWS domain (the mncs_nt1 account). This will allow the necessary drive mappings to be established without requiring a trust relationship between domains.

The permissions applied to the shared resources on the target servers (both share permissions and NTFS permissions) will need to be changed as well. As outlined in Table 2, the permissions are currently granted to the AMSMARKET_NEWS\mncs_nt1 account (or the global group to which it belongs). These will need to be modified to grant access to the *LOCAL* version of this account (e.g. SWASHXX1771L\mncs_nt1). During the transition period, permissions can be granted to both, so that when the target servers (e.g. the staging server and Backweb servers) are removed from the AMS_INTERNET domain, the change will be seamless.

REMOVAL OF THE NETBEUI LAN

The drive mappings currently in place traverse the NetBEUI LAN. Since the NetBEUI LAN will eventually be removed, these drive mappings will need to be reconfigured to utilize the TCP/IP network (**Figure 7**).

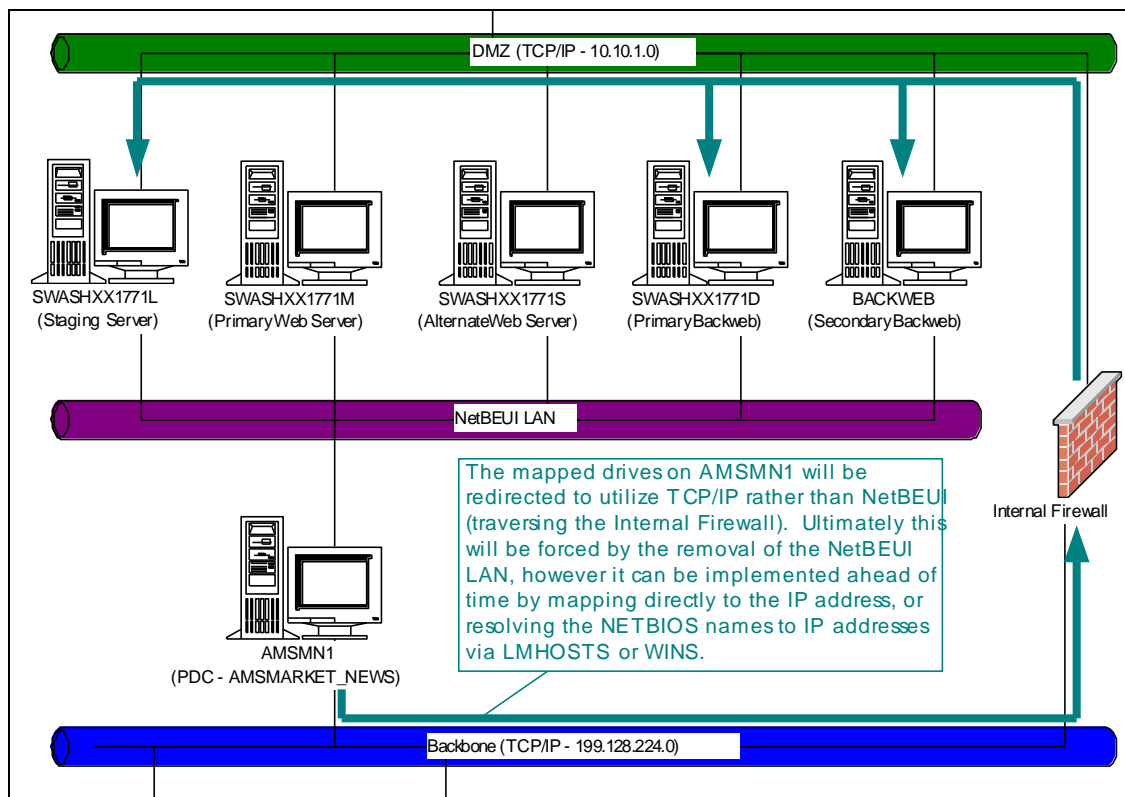


Figure 7: New SERVERX process

Although the Internal Firewall has been in place for several weeks, the only method for resolving NETBIOS names in the current configuration is by broadcast over the NetBEUI LAN.

There are two ways that this can be modified. First, the drive mappings can be reconnected and pointed directly at the target IP address. For example, the "L:" drive on AMSMN1 is currently mapped to \\SWASHXX1771L\\Day1. This drive mapping can be re-created to point to \\199.128.224.174\\Day1, which is the *internally* translated IP address of the staging server. The data will still arrive at the same location (the staging server), but in the second case it will utilize the TCP/IP network and traverse the Internal Firewall as opposed to the NetBEUI LAN.

The second method for directing traffic through the TCP/IP segment would be to provide for an alternate method of NETBIOS name resolution. Currently, the NETBIOS names of DMZ servers cannot be resolved by machines on the backbone. TCP/IP Broadcasts will fail (since the DMZ machines are on a separate segment), and there are no WINS entries for the DMZ servers. Adding entries to the LMHOSTS file on the AMSMN1 and 2 servers would allow the server names to be resolved, as well as adding static entries to the WINS database.

4. The drives on AMSMN1 which are currently mapped to the “L” server (H, L, and M) would be remapped to the new server’s shares.
5. The replication jobs that currently exist on L for replicating “Web-BBS” and “mncs” would need to be recreated on the new server.
6. The Internal Firewall Policy would need to be modified to allow for Site Server Content Replication to pass from the new server to the web servers (TCP Port 507).

USDA Document Delivery System

This USDA Document Delivery System is an augmented ‘push technology’ client/server program that allows the downloading and processing of USDA text files during one’s internet connection’s idle time using server software from BackWeb Technologies. The purpose of this system is a reliable, affordable, timely, and secure transmission medium.

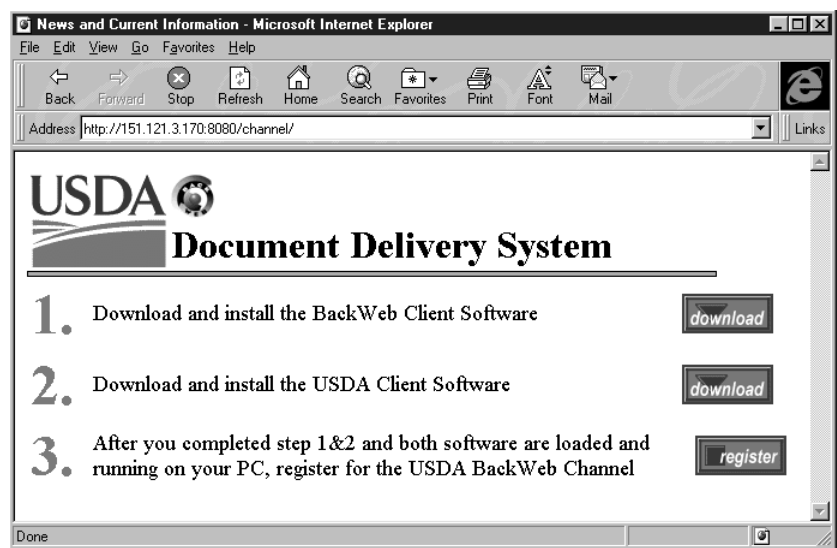
Please find and follow the instructions to properly install the ‘client’ end of this client/server application. **Since this system is based on a client/server model, each end-user must have the ‘client’ installed and running in order to receive files/data from the ‘server’ (USDA).** Text files are automatically saved locally in a subdirectory of your choice (such as c:\usda) and will require no change in the way you currently view or process these files, beyond the point of delivery.

Installation

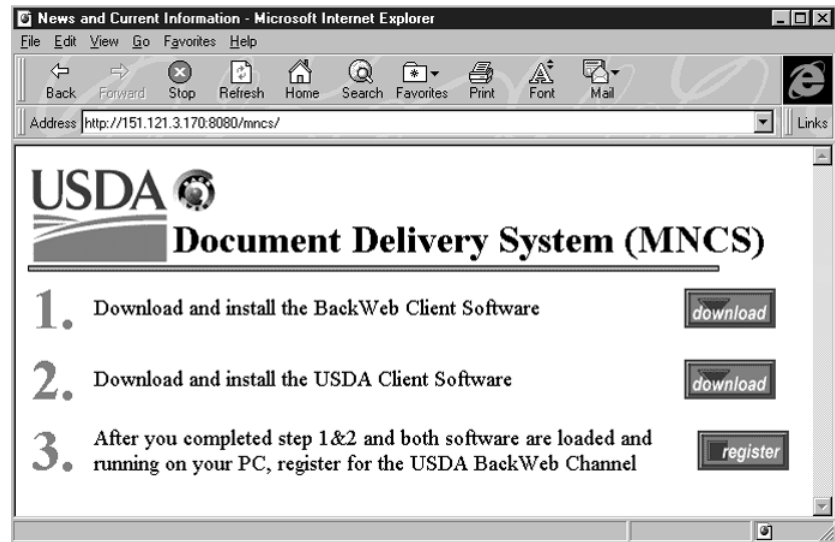
Installation is broken into five easy steps. Once step five is completed, the program will automatically begin working. It is important for optimal performance, that the steps below be followed in sequence. Depending on the speed and bandwidth of you internet connection, the installation process should not take more than 30 minutes, including all download time. The process for both private subscribers and AMS Market News sites is the same; except for the directory.

1. Use your internet browser to connect to: <http://151.121.3.170:8080/mncs>

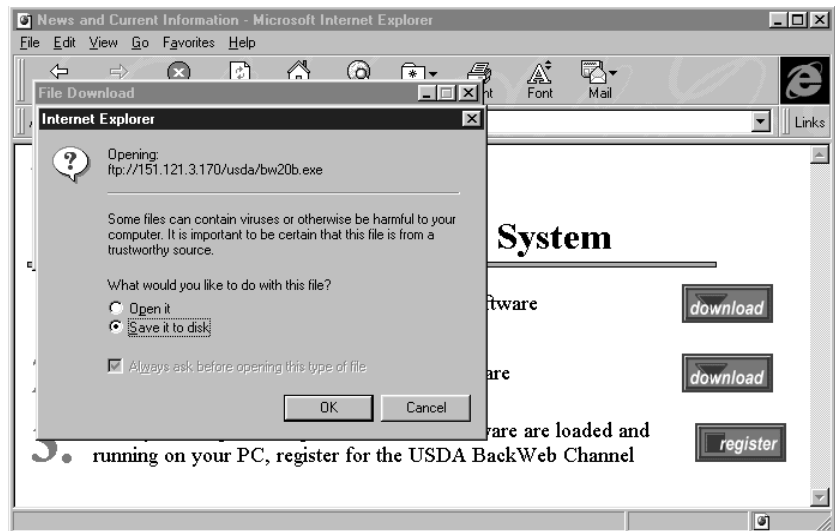
(Private Subscribers see this)



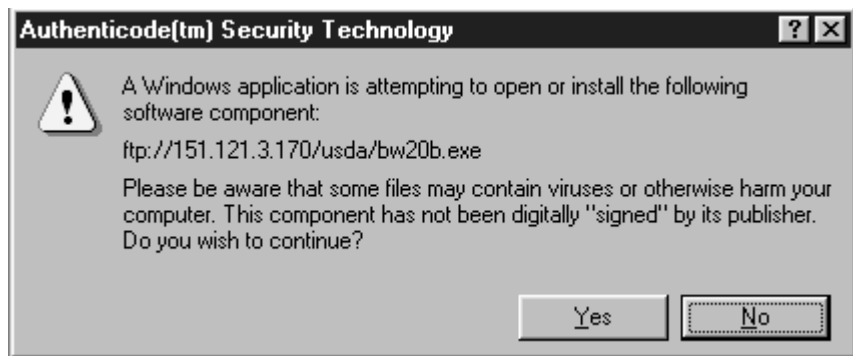
(AMS Employees see this)

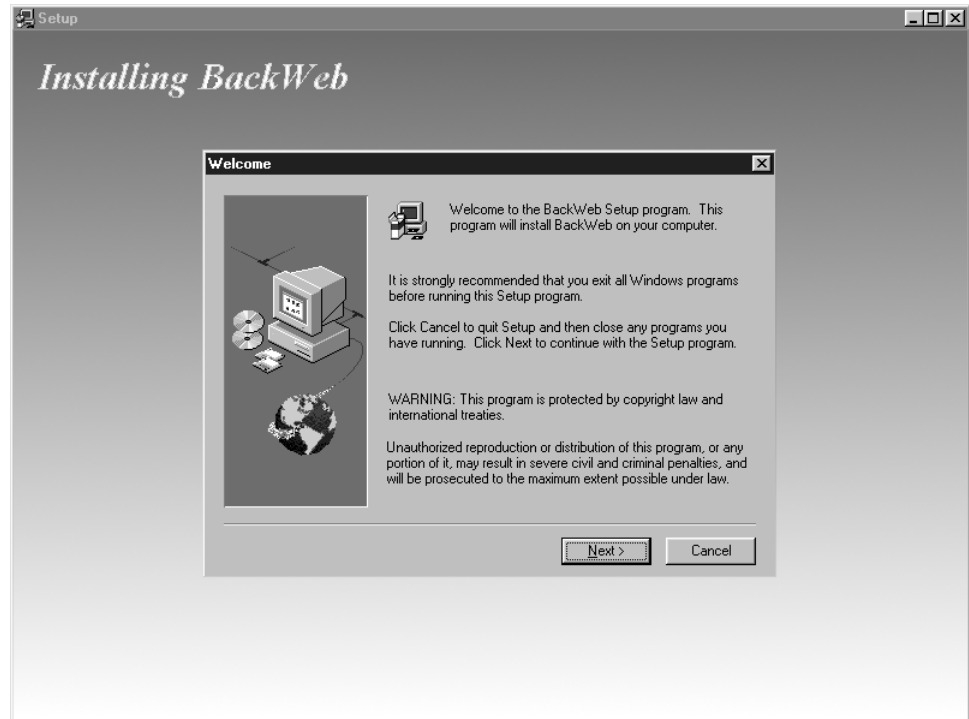


2. Click on the first "Download" button to download the BackWeb Client software. Depending on which web browser you are using, it may ask for the subdirectory in which to download it OR it may first ask you to either "open" or "save to disk". It is suggested that if you are not familiar with downloading files off the internet that you accept the subdirectory name already given and select "open" if asked. [Selecting "open" will allow the installation to start as soon as the download is completed.] If you were not given the "open" option prior to download, you must doubleclick on the file [in the subdirectory in which you downloaded the file] in Windows Explorer to install it.

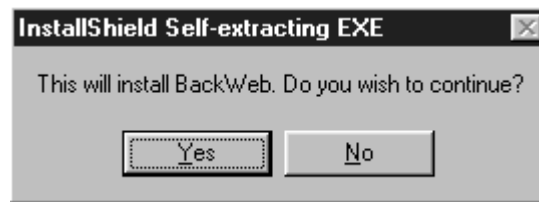


After saving the document to disk, Internet Explorer may warn you about a digital signature. Click on **YES** to continue the installation process.





Follow the installation prompts.

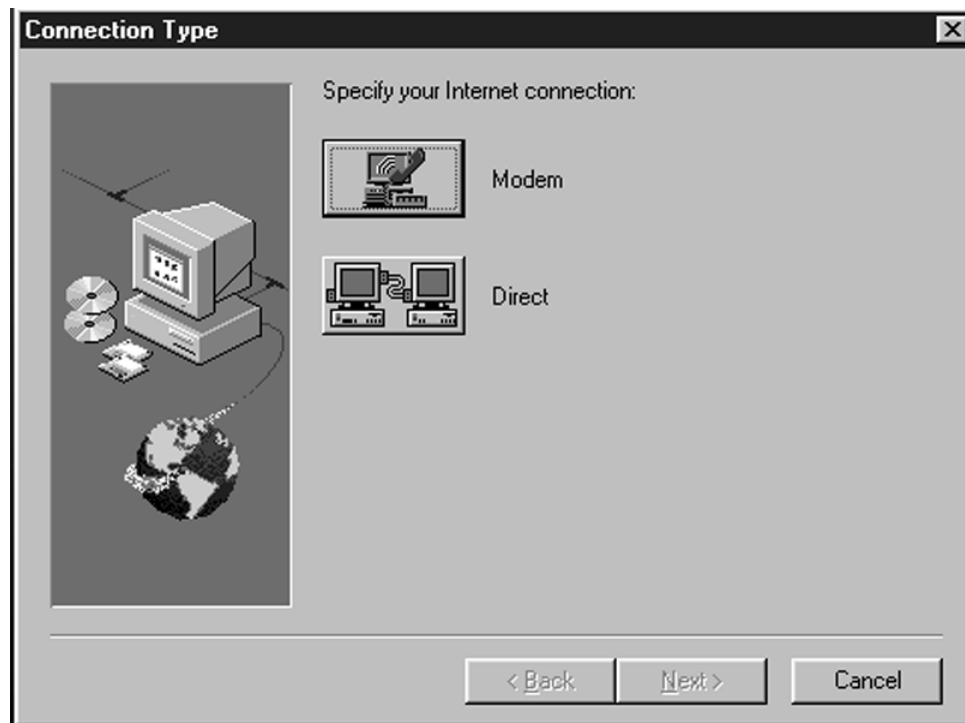




In the connection type choice, you will choose the "**Modem**" as your type of connection.

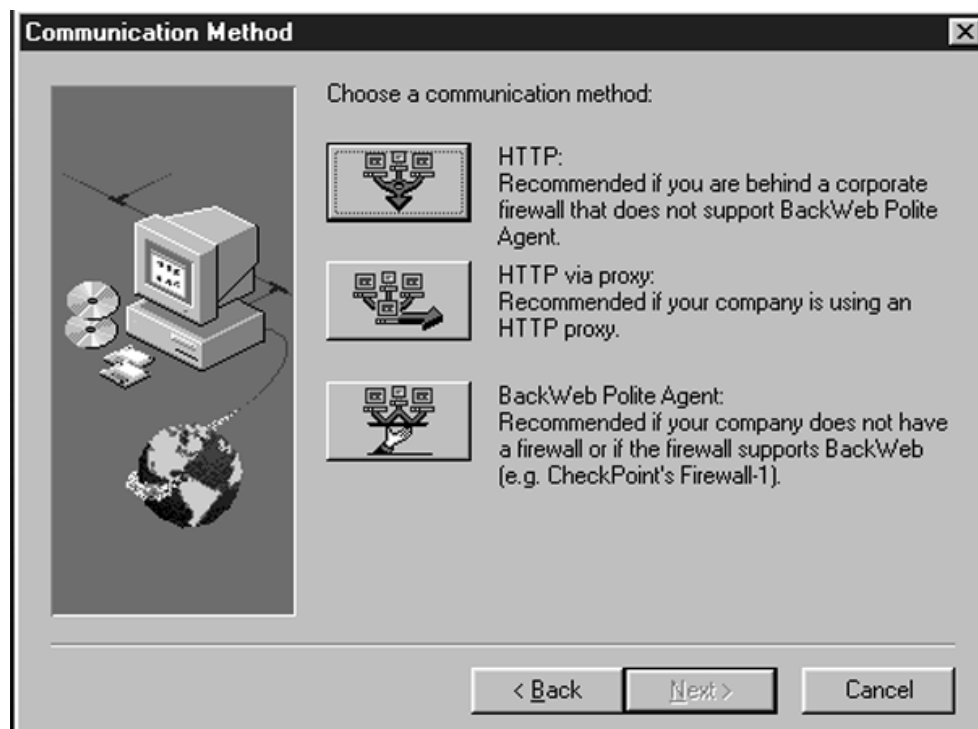
If you have a direct network connection, you will choose the "**Direct**" option.

Each option will continue the installation process.



If you chose the "**Direct**" connection method, you will be presented with the choices on the right.

Choose the bottom option "**Backweb Polite Agent**". Choose "**Next**" to continue with the Backweb Client installation.



If you chose the "**Modem**" connection method, the Backweb Quick Setup will begin.

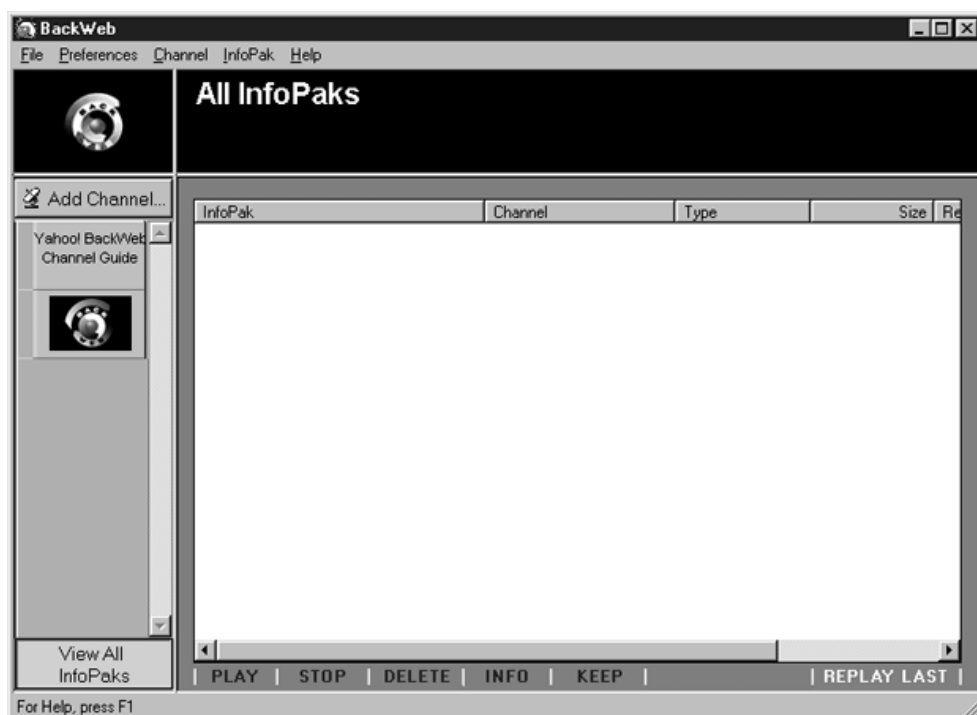
Choose "**Next**" to continue with the Backweb Client installation, accepting default settings, and finally ending the process by clicking on the "Finish" button



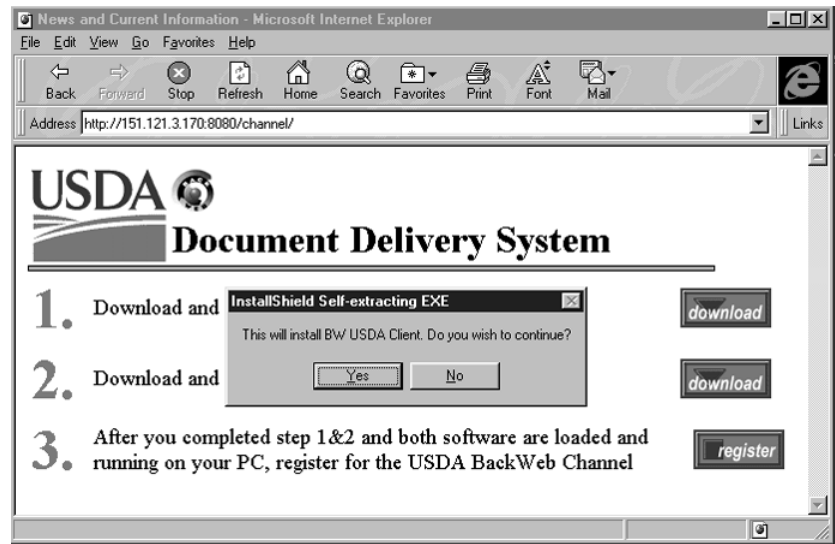
When the Quick Setup is complete, the final Backweb Client will appear.

You are now ready to proceed to "**Step 2**" in the Backweb installation process-- USDA Client Install.

Return to your Internet Explorer



3. Click on the second "**Download**" button to download the USDA Client software. Depending on which web browser you are using, it may ask for the subdirectory in which to download it OR it may first ask you to either "open" or "save to disk". It is suggested that if you are not familiar with downloading files off the internet that you accept the subdirectory name already given and select "open" if asked. [Selecting "open" will allow the installation to start as soon as the download is completed.] If you were not given the "open" option prior to download, you must doubleclick on the file [in the subdirectory in which you downloaded the file] in Windows Explorer to install it.



The BackWeb USDA Client Install process does four things:

- Asks for User Information (**Enter your Office location here**)
- Asks you to Designate a Destination Location (select the default)
- Creates Program Folders
- Copies Files (registering files and creating icons)

You should be here!

Click on "**Yes**" to install the USDA Client.



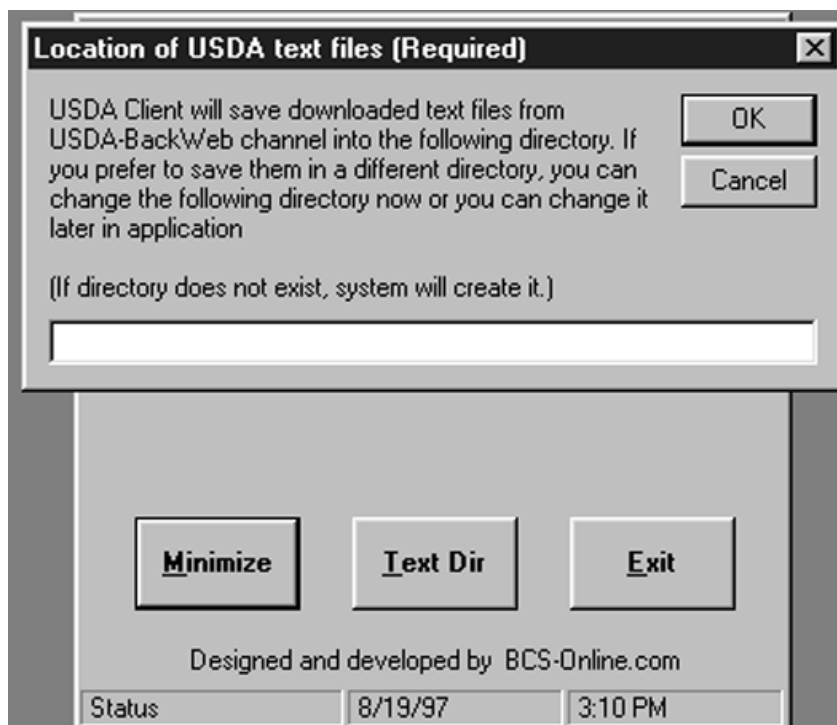
On the USDA `Client' software interface (shown above), Three separate buttons allow you to minimize the program, change the subdirectory where files from the USDA `Server' are saved locally on your machine, or manually shut down the system from receiving further files.

Minimize button: Clicking on this button will minimize the screen. To maximize, click on the BW-USDA client on the task bar.

TextDir button: Indicates the location of the USDA text files to be downloaded on your PC. Default directory is c:\USDA but you can change the default to any directory of your choice. If the subdirectory does not exist, the system will create it for you.

Exit button: Exiting from the application will stop the program and the files coming in from the USDA channel will not get processed until you run the client software again. The final prompt asks you to designate a directory for your pushed files.

Choose the default and click "OK" to complete the USDA Client Installation.



4. Once the installation is complete, the program will look for the USDA channel. Since the USDA channel is not present yet, the program will wait for you to subscribe to it. The process will continue as soon as you subscribe to the USDA channel.

5. To subscribe to the USDA channel, click the "REGISTER" button in your **internet browser**. The system prompts you to enter some personal information before subscribing you to the USDA

channel.

***If after following all five steps in sequence, new files are not being created within 5-10 minutes, the system is not working and installation should begin again, starting with Step 1.**

As soon as the installation is completed, the program will run on its own without further effort on your part. The USDA application gets launched every time the computer is turned on and runs continuously while the computer is in use, unless the application is shut down manually.



U.S. DEPARTMENT OF AGRICULTURE

Agriculture Marketing Service



BackWeb Server Installation Procedures



Evergreen Information Technology Services, Inc.
6475 New Hampshire Avenue
Suite 400
Hyattsville, Maryland 20783
Tel. 301.270.6200
Fax. 301.270.8167



Internosis
4301 North Fairfax Drive
Suite 650
Arlington, Virginia 22203

TABLE OF CONTENTS

Introduction	1
Hardware	2
Software.....	2
Operating System.....	2
Domain Membership	2
Windows 2000 Components.....	2
Windows 2000 Users and Groups	3
Files and Shares	3
IIS Configuration.....	4
Port Configuration	4
Virtual Directories.....	4
ISAPI Mappings	5
Additional Software	12
BackWeb Server	12
BackWeb Console.....	19
BackWeb Automation SDK.....	19
BackWeb Configuration.....	20
BackWeb Server License	23
Custom Package Importer (Perl Script)	26
Scheduling the PERL script.....	27
Channel Registration Page.....	31
File Installation	33
ODBC Configuration	34
MIME Type Configuration.....	35
BackWeb Failover	38
Appendix A: Installation Checklist.....	39
Version Control	41

INTRODUCTION

This document outlines procedures for installing and configuring a BackWeb Server for use in the Market News Communication System (MNCS). Step by step procedures for the installation of Windows 2000 are not specifically included, however relevant configuration items are recorded (e.g. required Windows 2000 components). Please reference the Market News Windows 2000 Server Installation documentation for more detailed procedures for Windows 2000 installation.

The specific hardware configuration listed in this document is that of the newly built primary BackWeb server (put into production January 25th, 2002). These specifications are provided for reference only, and should not be considered a minimum baseline. A similarly configured server platform could be used to host a BackWeb Server, although specific configuration items (such as RAID configuration and partition information) may need to be altered accordingly.

HARDWARE

The new BackWeb server is built on a Compaq Proliant ML530 chassis, with the following components:

Number of Processors:	2
Processor Type/Speed:	Pentium 933 Xeon
Memory:	896 MB
Hard Drives:	6 x 18 Gig SCSI Ultra3
RAID Configuration:	2 drives configured as RAID 1 (Mirrored) 4 drives configured as a RAID 5 Logical Unit

The Operating System is installed on the first Logical Unit (Mirrored) while the Second Logical Unit is used for data storage (specifically the `mkt_news` directories)

SOFTWARE

OPERATING SYSTEM

Operating System:	Windows 2000 Advanced Server
Updates:	Service Pack 2
	Q282522
	Q301625
	Q302755
	Q299796
	Q276471
	Q285851
	Q296185
	Q299553
	Q299687
	Q302755
	Q292435
	Q298012
	Q252795
	Q307454

Note: Since the installation of the first BackWeb server, Microsoft has released the Windows 2000 SP2 Security Rollup Hotfix, which includes all the necessary hotfixes above.

Domain Membership

The BackWeb Server should be installed as a stand-alone server (not a member of any domain).

Windows 2000 Components

Several of the Windows 2000 system components which are installed by default are not necessary for operation. The following list specifies which components should be installed on the BackWeb Server (changes to the default are marked with an *):

• Accessories and Utilities	Installed
• Certificate Services	Not Installed
• Indexing Service	Not Installed *
• Internet Information Service	Partially Installed *
○ Common Files	Installed
○ Documentation	Not Installed *
○ File Transfer Protocol (FTP) Server	Not Installed
○ Front Page 2000 Server Extensions	Not Installed *
○ Internet Information Services Snap-in	Installed
○ Internet Services Manger (HTML)	Not Installed *
○ NNTP Service	Not Installed
○ SMTP Service	Not Installed *
○ Visual Interdev RAD Remote Deployment Support	Not Installed
○ World Wide Web Server	Installed
• Management and Monitoring Tools	Not Installed
• Message Queuing Service	Not Installed
• Networking Services	Not Installed
• Other Network file and Print Services	Not Installed
• Remote Installation Services	Not Installed
• Remote Storage	Not Installed
• Script Debugger	Installed
• Terminal Services (Remote Administration Mode)	Installed *
• Terminal Services Licensing	Not Installed
• Windows Media Services	Not Installed

Windows 2000 Users and Groups

For the Market News Communication System to work properly, the BackWeb server needs to be configured with a specific account. A local user called “mncs_nt1” needs to be created. This user should be a member of the “Administrators” group, and must have the same account name and password as the “mncs_nt1” account in the “AMSMARKET_NEWS” domain.

Files and Shares

The second RAID Logical Unit (formatted as the F: partition under Windows 2000) is used to store the `mkt_news` directories. The following configuration should be used for these directories:

- The partition used for the F: drive should be formatted with NTFS
- The NTFS Permissions on the root of the F: drive should be assigned as follows:
 - Administrators: Full Control
 - SYSTEM: Full Control
- The `mkt_news` and `mkt_news2` directories should be created in the root of the F: drive
- The `mkt_news` and `mkt_news2` directories should be shared (with the same names).
- The share permissions for both directories should be:

- Administrators: Full Control
- SYSTEM: Full Control

Note that the “mncs_nt1” account should be a member of the “Administrators” group, and therefore will have the necessary access to these directories.

IIS CONFIGURATION

Changes to the default configuration of the Internet Information Service (IIS) are required both to allow interoperability with BackWeb, as well as to ensure the secure configuration of the server.

Port Configuration

The BackWeb server will listen for client connections on TCP port 80. This is also the default port assigned to the Default Web Site in IIS. In order to prevent both applications from competing for port 80, IIS needs to be configured to listen on a different port (TCP port 8080 will be used for this).

Open the “Internet Information Services” Snap-In (by selecting “Start | Programs | Administrative Tools | Internet Services Manager”) and expand the tree to locate the Default Web Site. Right click on the Default Web Site and select “Properties.”

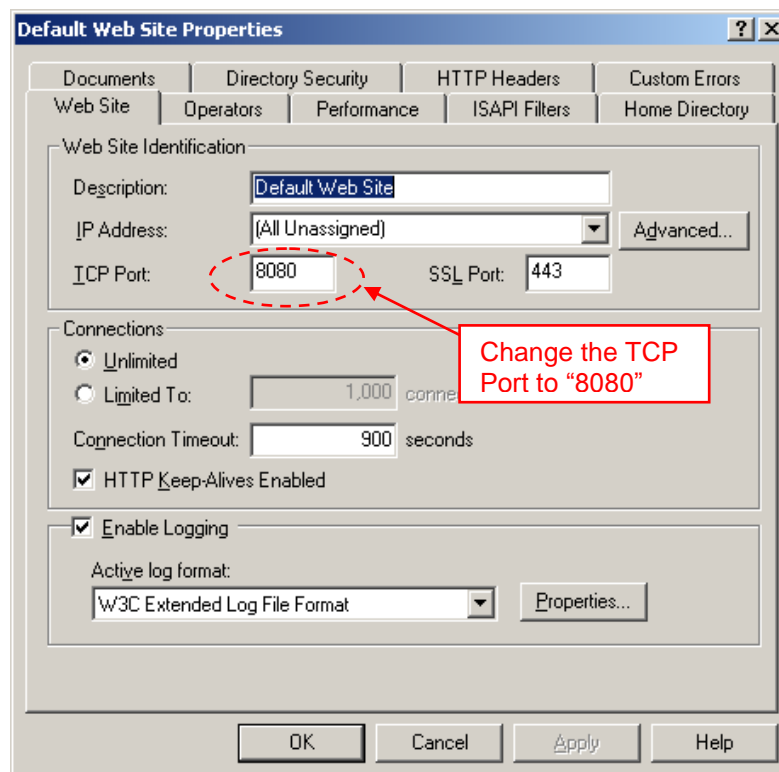


Figure 1: IIS Port Configuration

In the “TCP Port” box, change the value from the default of “80” to “8080” (Figure 1).

Virtual Directories

There are a number of virtual directories that are installed by default upon IIS installation. Most of these virtual directories are not necessary and can be a security

risk. The following virtual directories (located under the Default Web Site) should be deleted (right click on the Virtual Directory and select “delete”):

IIS Admin	IIS Help	Scripts	IIS Samples	MSADC
-----------	----------	---------	-------------	-------

The following NTFS directories should also be deleted (if they exist, they will be located beneath C:\inetpub\wwwroot):

_private	_vti_log	_vti_cnf	_vti_pvt	_vti_script
----------	----------	----------	----------	-------------

ISAPI Mappings

IIS is installed with a number of Internet Service Application Programming Interfaces (ISAPI) mappings installed by default. These mappings direct IIS to utilize certain DLLs to process requests for files with a given extension. Some of these DLLs are known to have security vulnerabilities, and as a general rule any unnecessary ISAPI mappings should be removed. To manage ISAPI mappings, open the Internet Information Service Snap-In, right click on the server in question and select “properties” (**Figure 2**). Note that by selecting properties for the *Server* vs. the *Default Web Site*, it will apply to any additional sites created on the server.

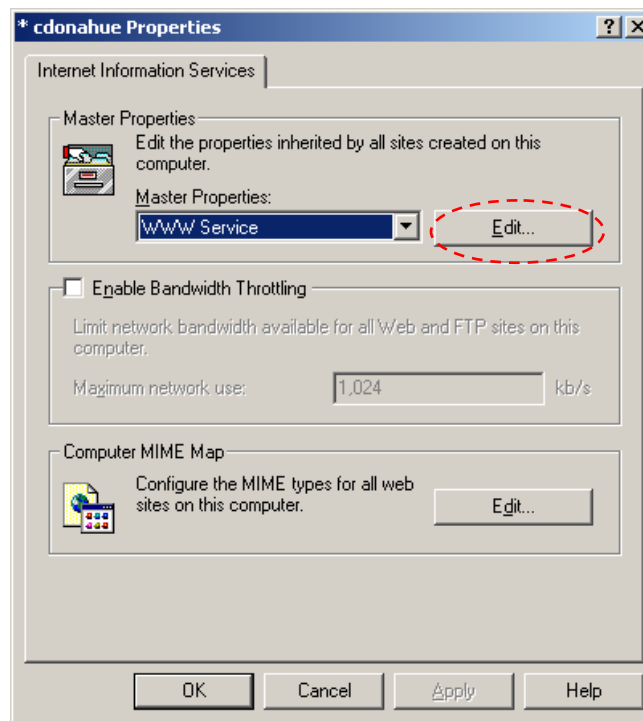


Figure 2: Server Properties

Under the master properties drop-down, ensure “WWW Service” is selected and click “Edit.”

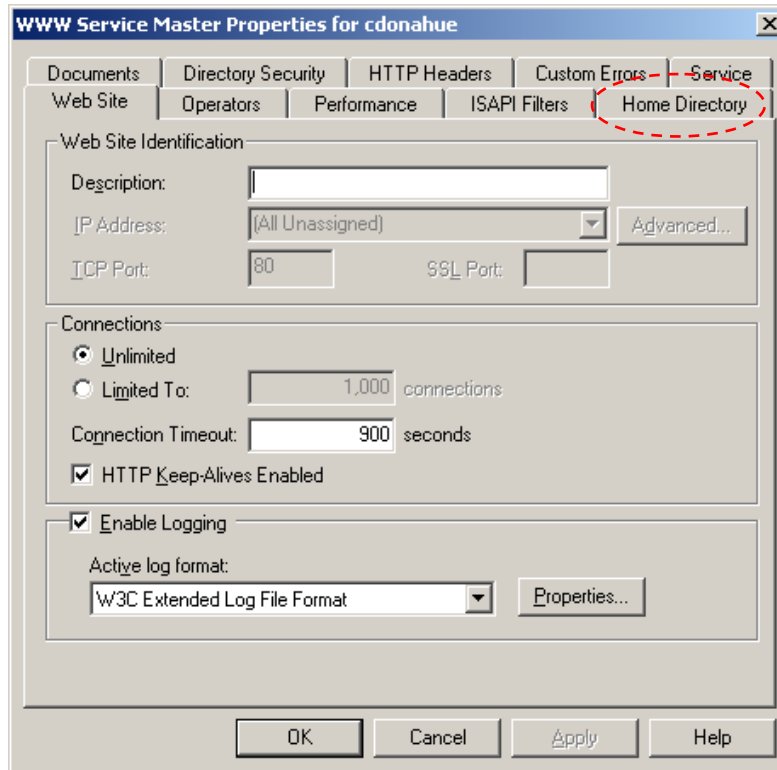


Figure 3: WWW Service Master Properties

This brings up the WWW service Master Properties dialogue (**Figure 3**). Select the "Home Directory" Tab.

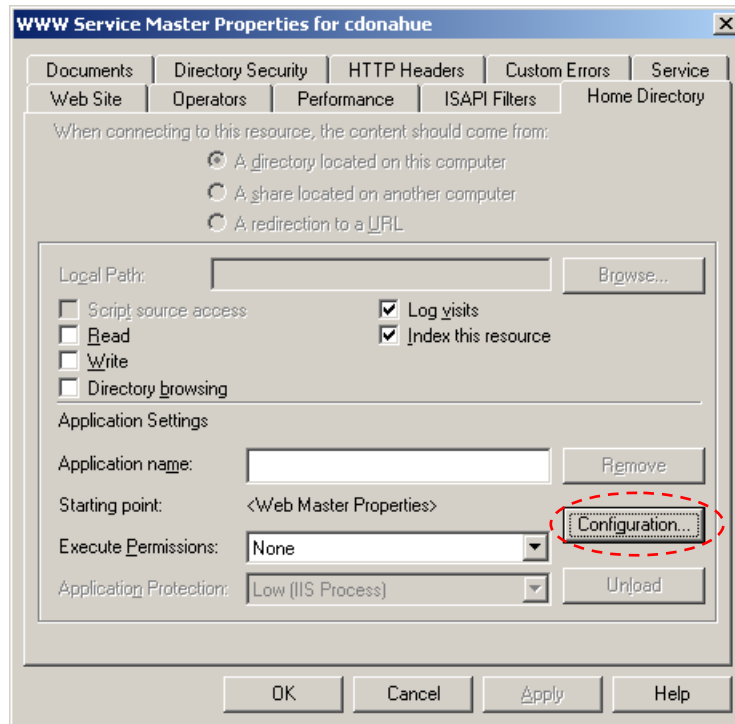


Figure 4: Home Directory Tab

In the lower-right corner of the “Home Directory” tab, click on the “Configuration” Button (Figure 4).

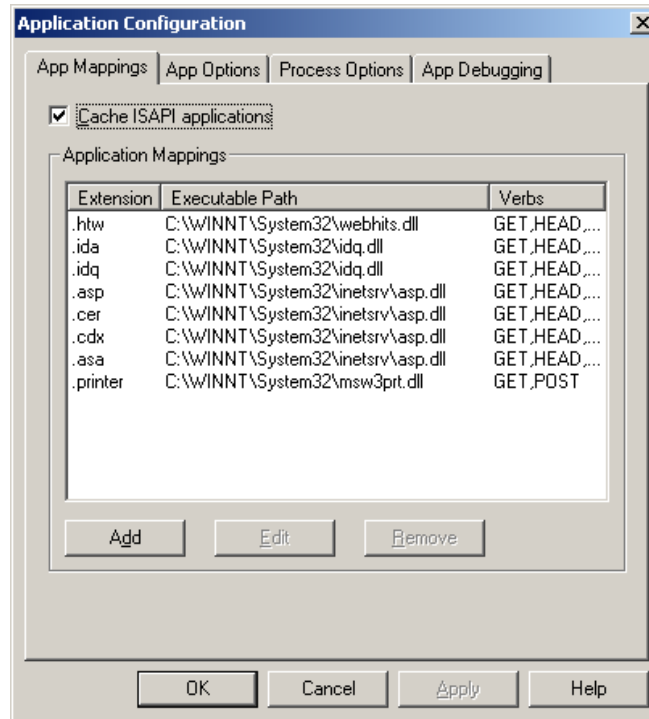


Figure 5: Application Configuration

The “Application Configuration” dialogue will display a number of ISAPI application mappings (**Figure 5**). The following ISAPI mappings should be removed (select the extension and click the “Remove” button):

.htw	.ida	.idq	.idc
.stml	.shtml	.stm	.htr

The only mappings that should remain are:

.asp	.cer	.cdx	.asa
------	------	------	------

Note that the **.printer** mapping is special. Although it can be removed here, if the server is restarted, Windows 2000 will recreate the mapping automatically. To remove the **.printer** mapping permanently, Web-based printing must be disabled. This must be done through the Group Policy Snap-In. Select *Start / Run* and type “MMC” in the “Open” box.

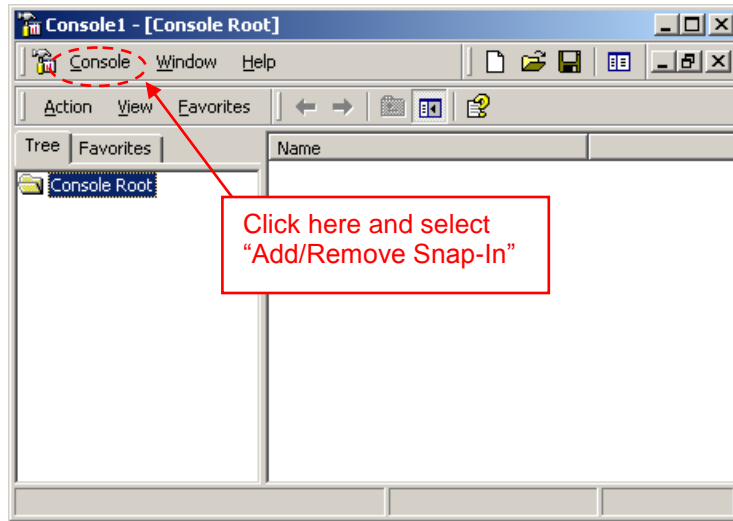


Figure 6: Microsoft Management Console

This will bring up the Microsoft Management Console (**Figure 6**). Click on “Console” (in the upper left hand corner of the window) and select “Add/Remove Snap-In.”

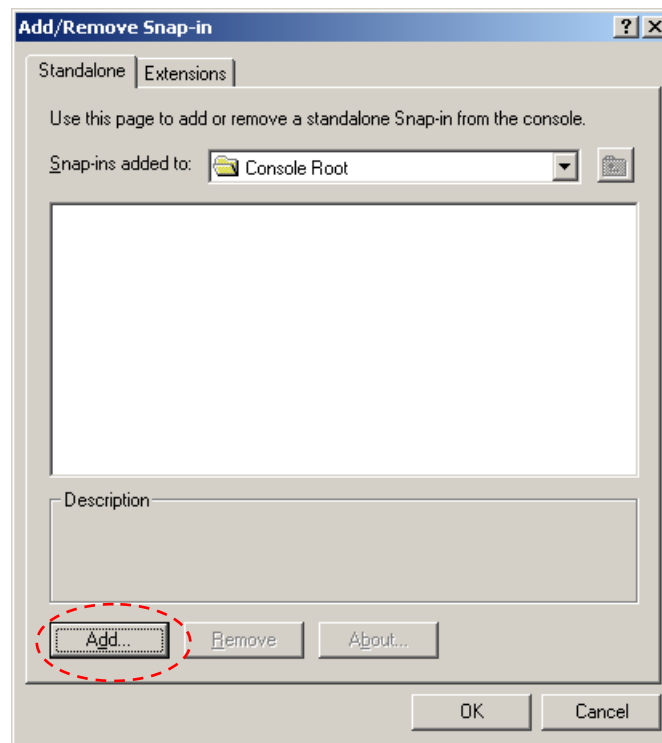


Figure 7: Add/Remove Snap-In

The “Add/Remove Snap-In” dialogue will be displayed (**Figure 7**). Click the “Add” Button to see a list of available Snap-Ins.

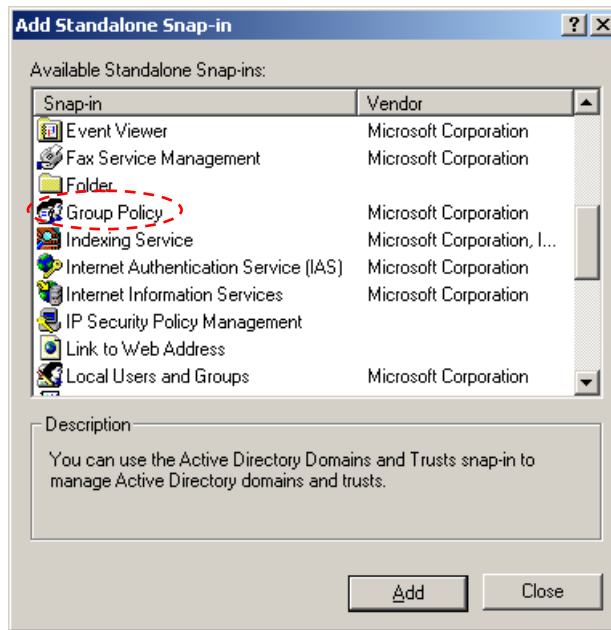


Figure 8: Add Snap-In

A list of available Snap-Ins will be displayed (**Figure 8**). Scroll down and select the “Group Policy” Snap-In and click “Add.”

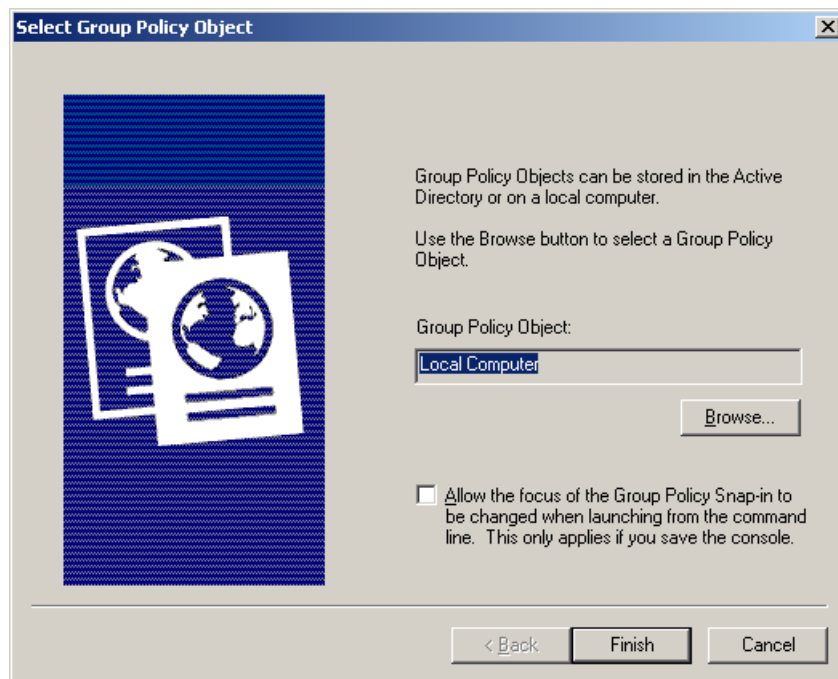


Figure 9: Select Local Policy

The Group Policy Snap-In will display a dialogue specifying which computer to target (**Figure 9**). The Local Computer should be selected by default. Click “Finish” and close the “Add Standalone Snap-In” dialogue. The newly added “Local Computer Policy” Snap-In should be displayed in the “Add/Remove Snap-In” dialogue. Click “Ok” to return to the MMC console.

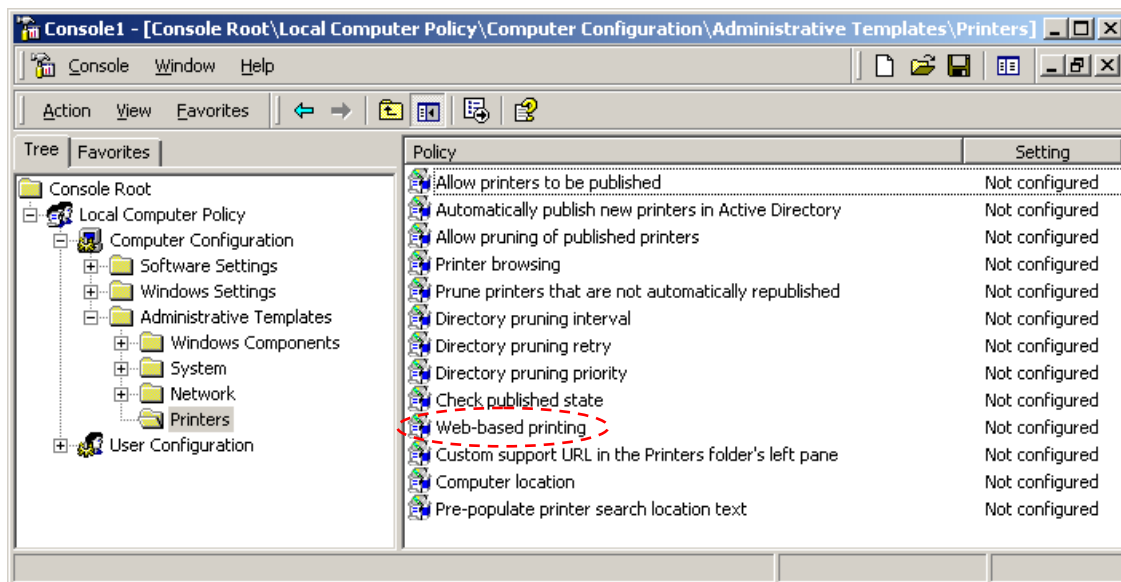


Figure 10: Local Computer Policy Snap-In

The “Local Computer Policy” should now be displayed under the Console Root. Expand it to display “*Local Computer Policy | Computer Configuration | Administrative Templates | Printers*” (**Figure 10**). Under the “Printers” folder, look for the “Web-based Printing” entry. Double-click this entry and select “Disabled.” When the server is restarted, the .printer mapping will no longer be created under IIS.

NOTE: *ISAPI mappings are sometimes recreated automatically if Windows 2000 components are added/removed from the system. If any Windows 2000 components are added or removed, the procedures for removing these ISAPI mappings may need to be performed again.*

ADDITIONAL SOFTWARE

The following sections list additional software components required for implementing USDA's Market News Communication System.

BackWeb Server

Inserting the "BackWeb Server" CD should automatically launch the Installation splash screen.

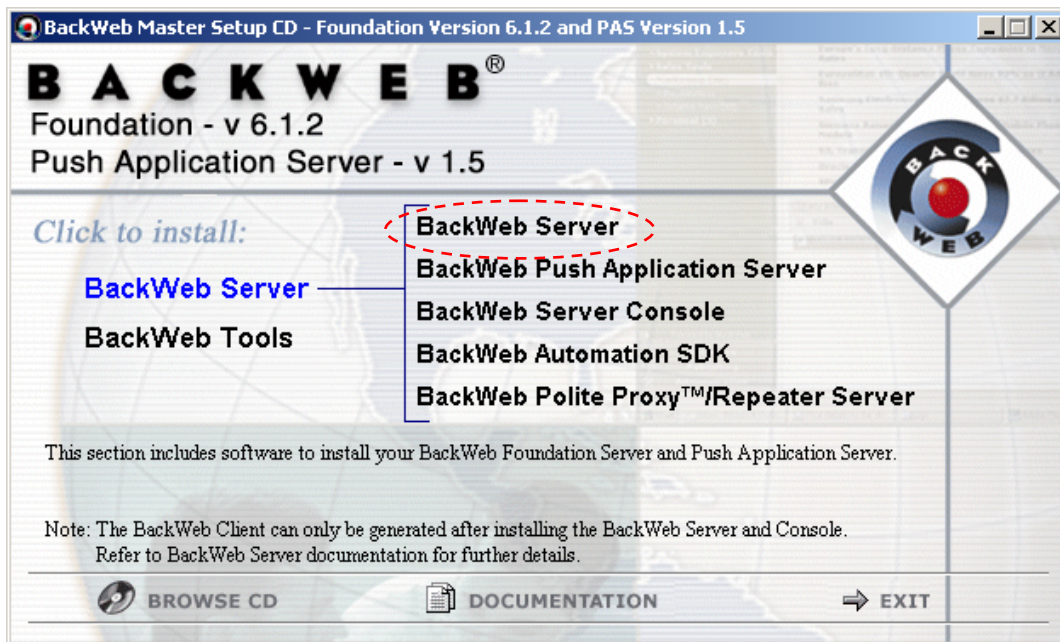


Figure 11: BackWeb Server CD Splash Screen

The BackWeb Server installation can be launched by expanding "BackWeb Server" and selecting the "BackWeb Server" link (**Figure 11**). A dialogue box will ask if you want to install BackWeb Server. Select "Yes" to begin the installation.

Note: If the splash screen does not launch when the CD is inserted, or the splash screen link does not launch the installation correctly, it can also be manually started by exploring the CD and running the \Server\Win\Setup.exe application.

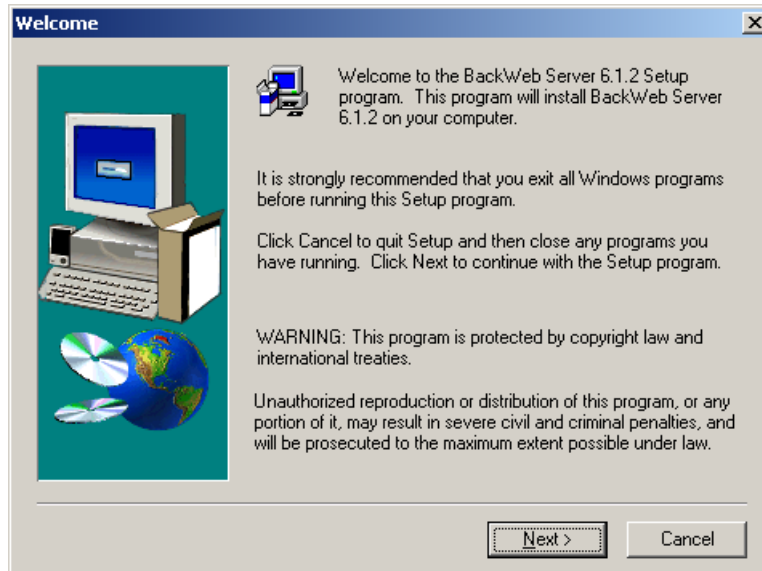


Figure 12: BackWeb Server Installation Welcome

The BackWeb Server Installation Welcome screen will be displayed (**Figure 12**). Click “Next” to continue.

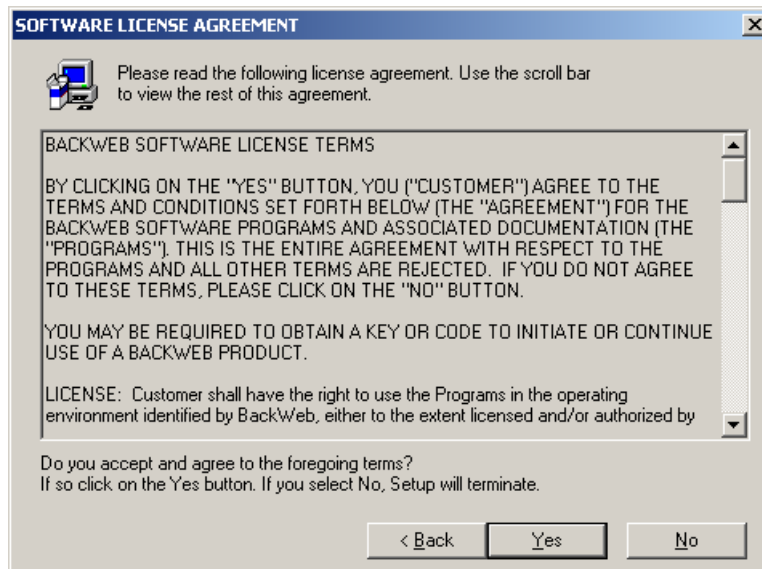


Figure 13: License Agreement

The Software License Agreement will be displayed (**Figure 13**). Click “Yes” to agree to the license terms and continue the installation.

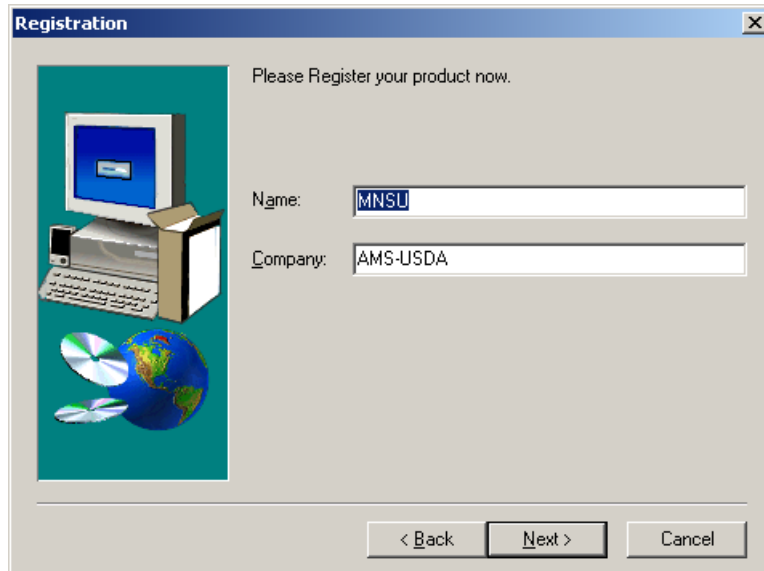


Figure 14: Software Registration

The Software Registration Page will be displayed (**Figure 14**). Enter an appropriate Name and Company and click “Next” to continue.

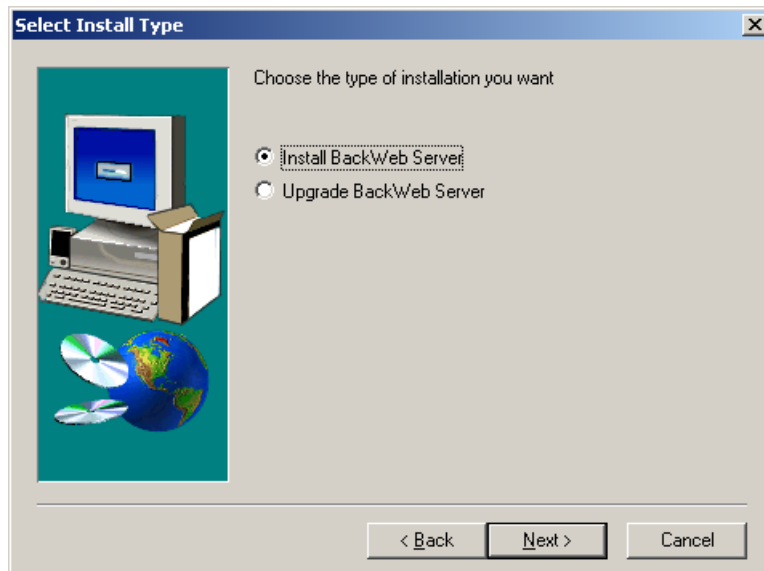


Figure 15: Installation Type

The “Install Type” selection will be displayed (**Figure 15**). “Install BackWeb Server” should be selected. Click “Next” to continue.

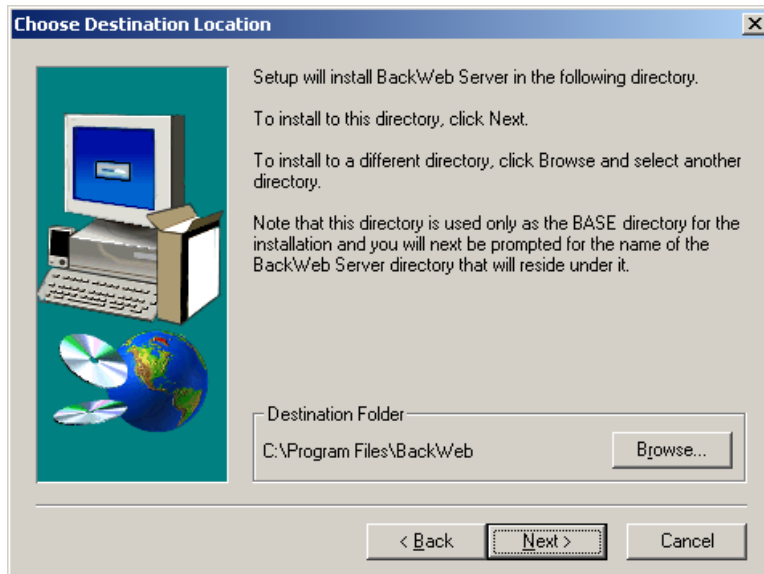


Figure 16: Program Files Location

The “Choose Destination Location” dialogue will now be displayed (**Figure 16**). If the program files will be installed in a different location, click “Browse” to select the desired location. Otherwise, click “Next” to accept the default location (C:\Program Files\BackWeb).

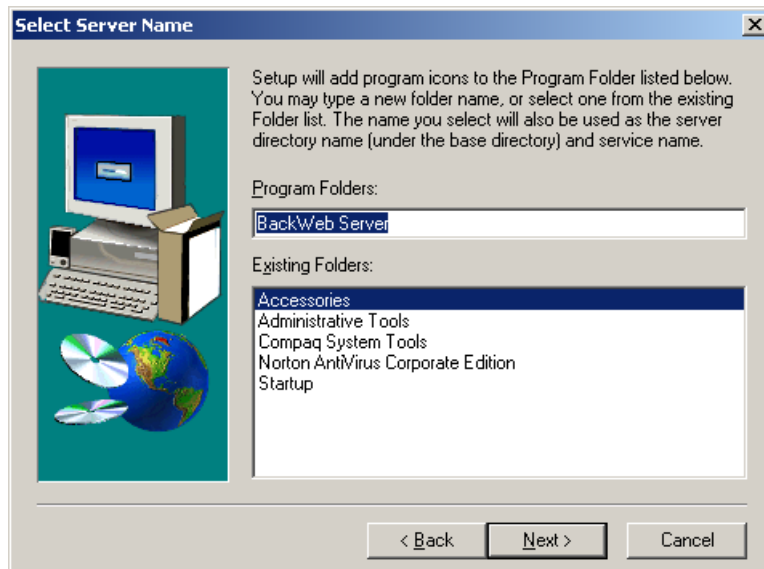


Figure 17: Start Menu Folder

The next dialogue will create a Program Folder with shortcuts on the Start Menu (**Figure 17**). Accept the default Folder Name (BackWeb Server) and click “Next” to continue.

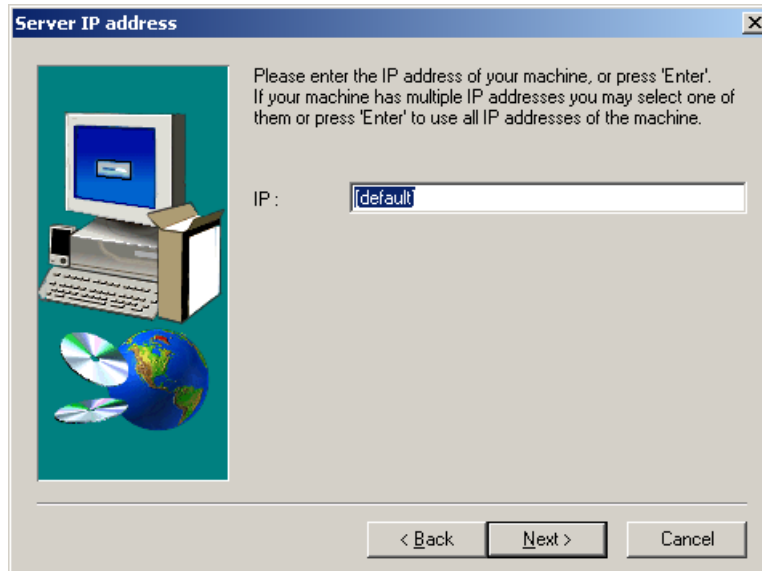


Figure 18: IP Address

The “Server IP Address” will now be displayed (**Figure 18**). This is primarily intended to limit which IP address(es) the BackWeb Server will bind to when running on a server with multiple Network Interfaces and/or IP addresses. The “[default]” setting will allow the BackWeb Server to bind to all IP addresses on the machine. Accept this default setting and click “Next” to continue.

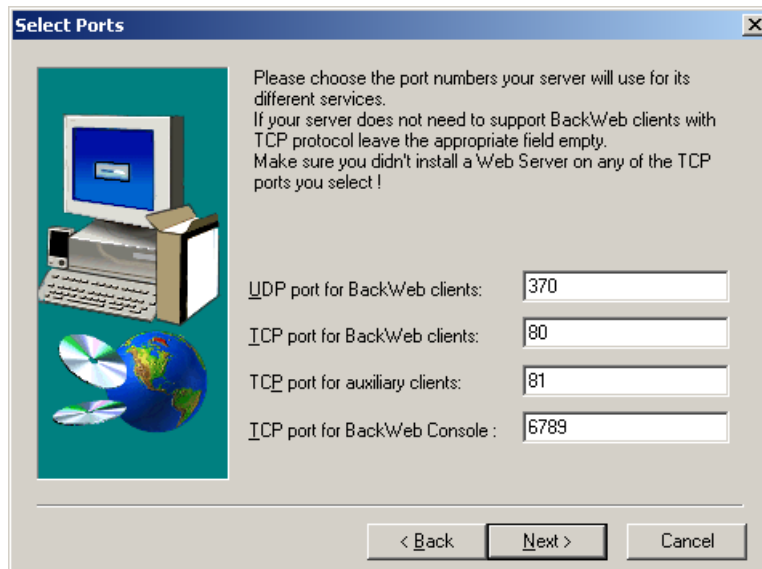


Figure 19: Application Ports

The “Port Numbers” dialogue box will now be displayed (**Figure 19**). Accept the default settings. Please note that the “Port Configuration” procedures with regard to IIS outlined earlier in this document should have already been implemented, otherwise you may receive an error message about port 80 already being in use. If the Port Configuration settings have not been implemented, cancel the installation and perform those procedures before continuing, otherwise click “Next” to proceed.

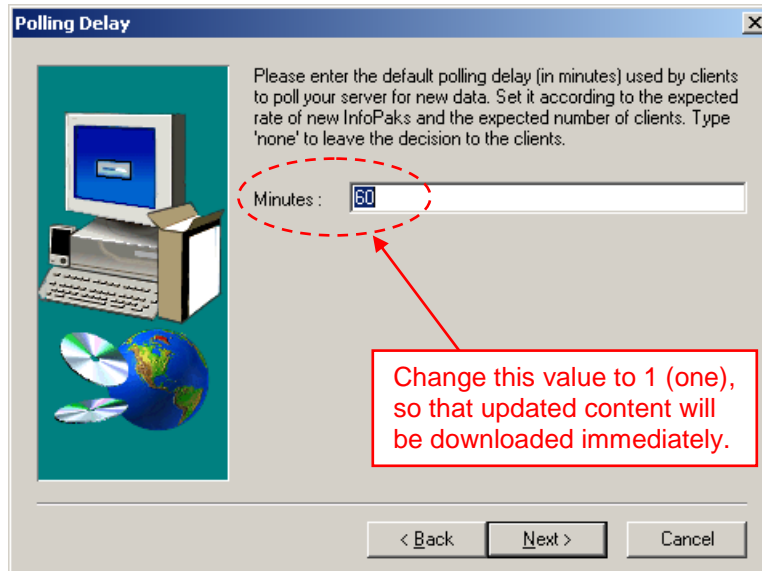


Figure 20: Polling Delay

The “Polling Delay” dialogue box will now be displayed (**Figure 20**). This setting determines how often a client connected to the server will poll for updated content. The default setting is 60 minutes. In order for the MNCS system to provide the timeliest response, this setting should be changed to 1 (one) minute. Once this has been modified, click “Next” to continue.

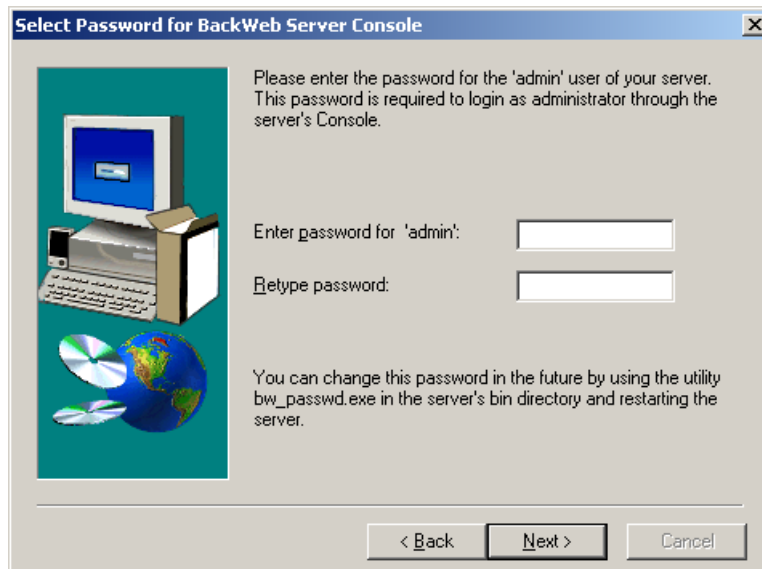


Figure 21: Admin Password

The “Admin Password” dialogue box will now be displayed (**Figure 21**). This password is used to control access to the BackWeb Console, both from the local machine, as well as from the network. Note that this password is completely unrelated to any local or domain passwords/accounts associated with Windows 2000 or NT. It **only** applies to access to the BackWeb Server Console. Enter an appropriate password here and type it a second time to confirm. Write down the password and store it in a secure location before clicking “Next” to continue.

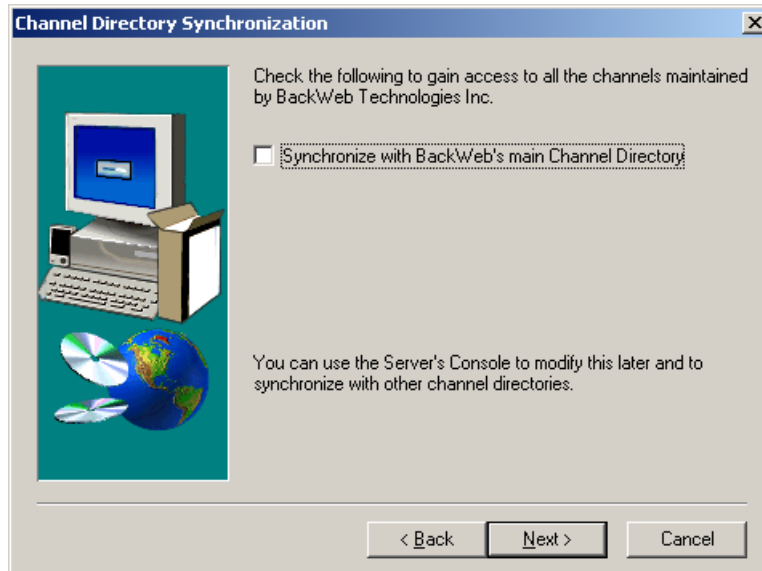


Figure 22: BackWeb Channel Directory Synchronization

The “Channel Directory Synchronization” dialogue box will now be displayed (**Figure 22**). This allows a BackWeb server to synchronize with BackWeb servers maintained by the BackWeb company, providing access to additional content. This is *not* required for the MNCS system, so leave the box unchecked and click “Next” to continue.

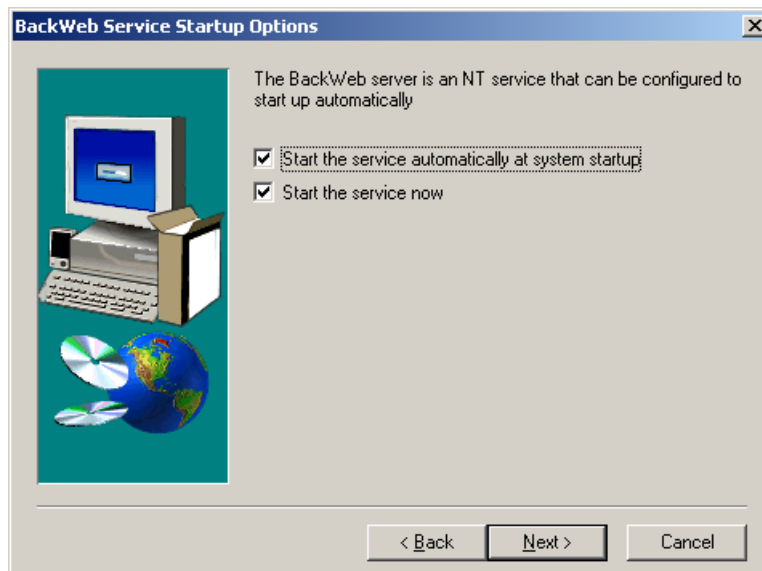


Figure 23: Startup Options

The “Services Startup Options” dialogue will now be displayed (**Figure 23**). Accept the default (both boxes checked), and click “Next” to continue.

The installation will now proceed to copy files and install the BackWeb Server software. Once the BackWeb Server installation is completed, proceed to the BackWeb Console installation.

BackWeb Console

The BackWeb Console software installation is extremely straightforward. It can be launched from the CD splash screen, or by exploring the CD and running the “\Console\Setup\Setup.exe” application. Accept all the default settings (the only modifiable entry is the Program Files location). Once the BackWeb Console installation is completed, proceed to the Automation SDK installation.

BackWeb Automation SDK

The BackWeb Automation SDK (Software Development Kit) includes libraries which are required for the MNCS system to function correctly. The installation can be launched from the CD splash screen, or manually by exploring the CD and running the “\AutoSdk\Win\Setup.exe” application.

Accept all the default settings for the SDK installation. The necessary files will be copied to the machine. At this point, the installation program will check for the existence of a PERL interpreter. If none is installed (which should be the case), it will display the following notice (**Figure 24**):

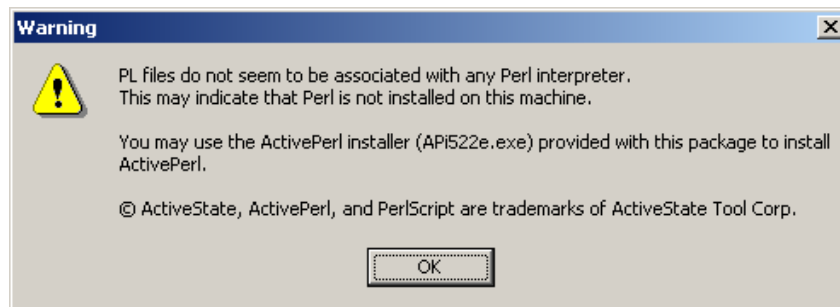


Figure 24: Perl Not Found

Click “Ok” to acknowledge the message. You will then be asked if you wish to install “ActivePerl,” a PERL interpreter distributed with the BackWeb software (**Figure 25**). Click “Yes” to initiate the ActivePerl installation.

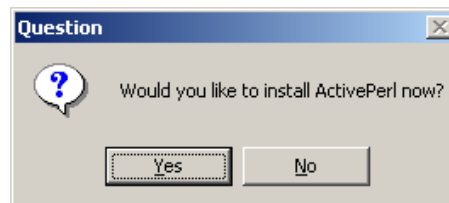


Figure 25: Perl Installation Prompt



Figure 26: Active Perl Installation Launch

The “ActivePerl” installation program will now be launched (**Figure 26**). Accept all the default settings for the ActivePerl installation. Once the ActivePerl installation is complete, the installation of the BackWeb Automation SDK will be complete (**Figure 27**).

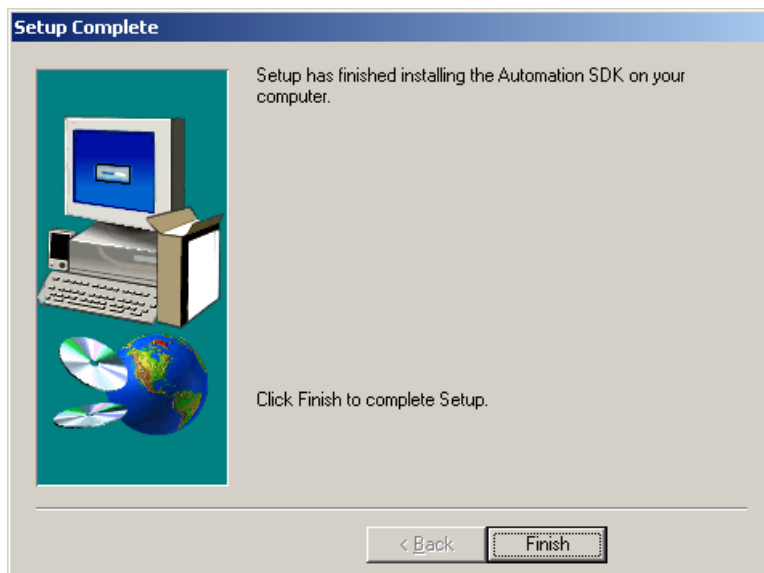


Figure 27: SDK Installation Complete

BackWeb Configuration

Once the BackWeb Server components have been installed, the USDA Sub-Channel and Satellite Exposure group need to be created to ensure correct operation of the MNCS system. To configure the BackWeb Server, you must connect to it through the Console. Open “*Start | Programs | BackWeb Console | BackWeb Console.*” You will see a logon screen, as illustrated in **Figure 28**.

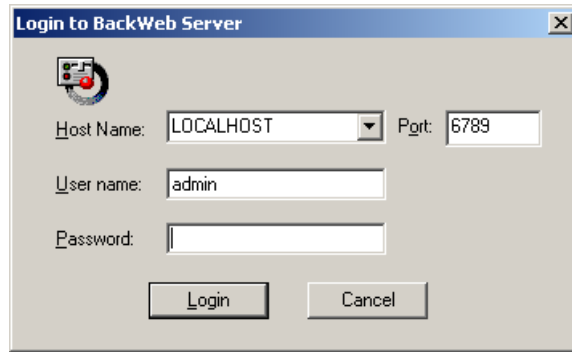


Figure 28: Connecting to Server Console

If you are connecting from the server itself, type in “Localhost” for the Host Name or enter the server’s IP address if configuring the server from a remote machine. Enter the password for the “admin” account (this is the password that was entered when installing BackWeb Server) and press “Login.” The console application should now connect to the server.

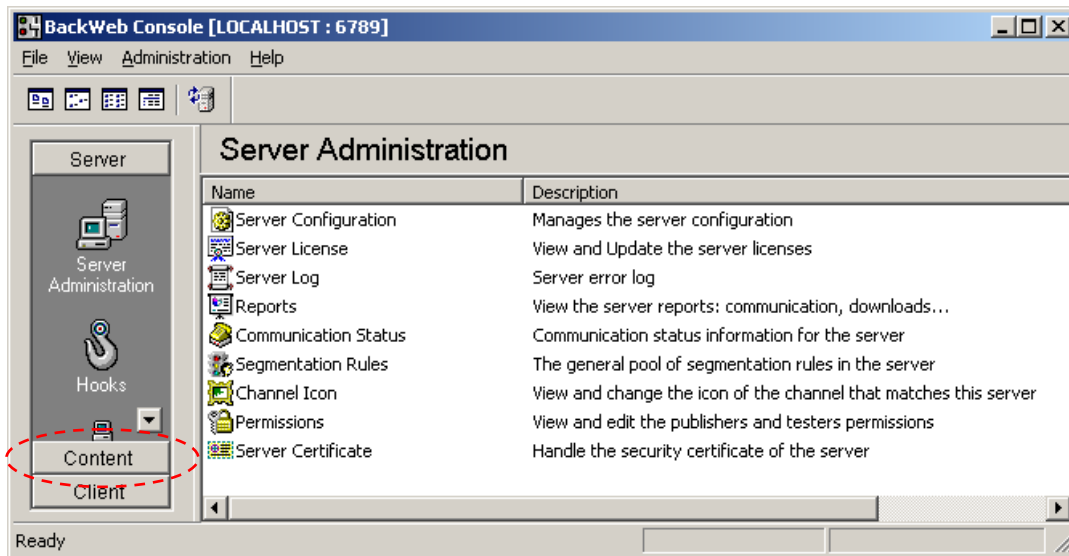


Figure 29: Server Administration

To manage Sub-Channels and Exposure groups, click on the “Content” tab in the navigation panel (**Figure 29**).

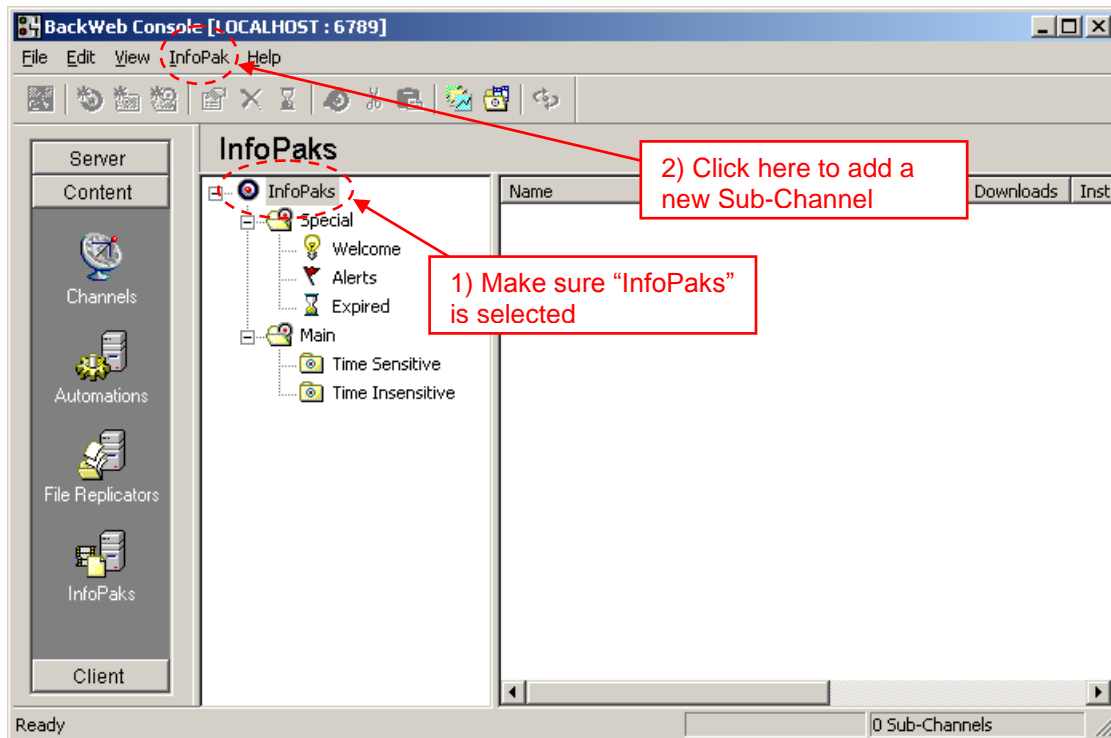


Figure 30: InfoPaks

Under the “Content” tab, click on “InfoPaks” (**Figure 30**). In the InfoPak tree, there should be two existing Sub-Channels (Special and Main). The custom PERL script that imports Market News Reports into BackWeb requires that a specific Sub-Channel (USDA) exists. Make sure that the root “InfoPaks” is highlighted, click on the “InfoPak” menu, and select “Add Sub-Channel.”

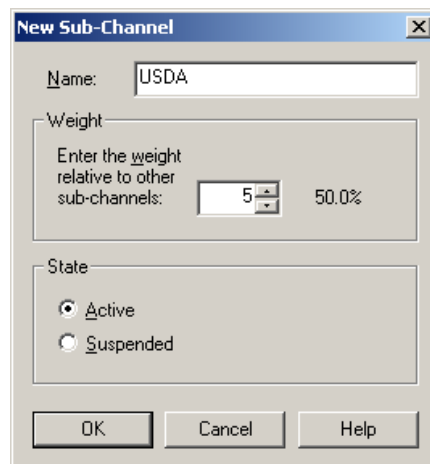


Figure 31: New Sub-Channel

This will bring up the “New Sub-Channel” dialogue box (**Figure 31**). Type “USDA” in the Name field. Accept all the other defaults and click “Ok.” You will be returned to the InfoPak screen. The “USDA” Sub-Channel should now appear in the tree.

The “Satellite” exposure group needs to be created under the USDA Sub-Channel. To do this, highlight the USDA Sub-Channel, click on the “InfoPak” Menu, and select “Add Exposure Group.”

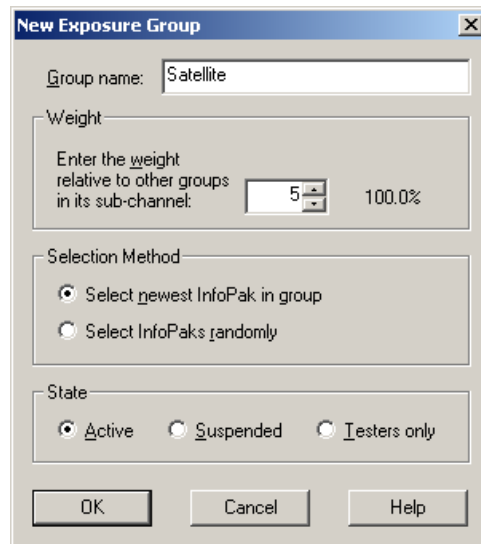
A screenshot of the "New Exposure Group" dialog box. The "Group name" field contains "Satellite". The "Weight" section has a text input "Enter the weight relative to other groups in its sub-channel:" followed by a numeric spinner set to "5" and a percentage display "100.0%". The "Selection Method" section has two radio buttons: "Select newest InfoPak in group" (selected) and "Select InfoPaks randomly". The "State" section has three radio buttons: "Active" (selected), "Suspended", and "Testers only". At the bottom are "OK", "Cancel", and "Help" buttons.

Figure 32: New Exposure Group

This will bring up the “Add Exposure Group” dialogue box (Figure 32). Type “Satellite” in the Group Name field. Accept all the other defaults and click “Ok.”

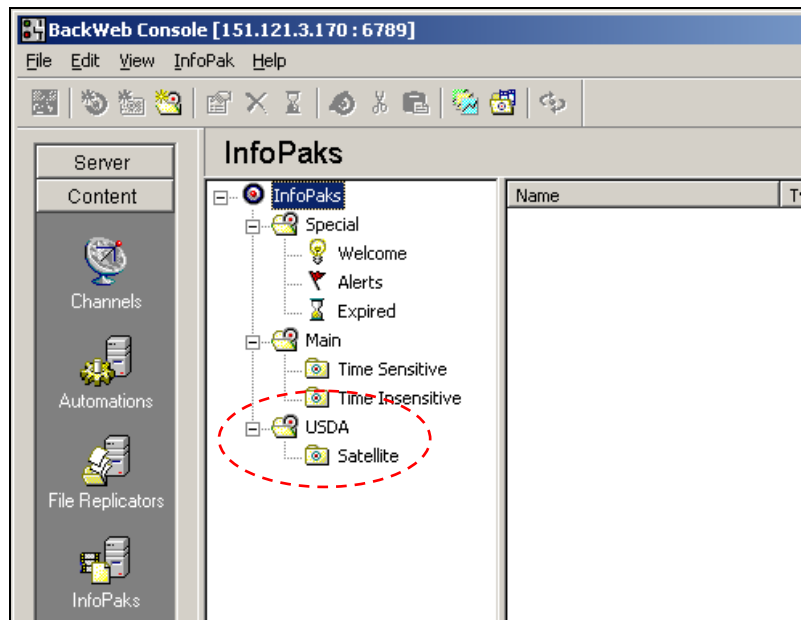


Figure 33: Sub-Channel and Exposure Group Created

You will be returned to the InfoPak screen. The newly created exposure group should now be visible in the tree (Figure 33).

BackWeb Server Host ID

When the BackWeb Server is installed, it will have an Evaluation License installed. This Evaluation License will expire in approximately a month, and must be replaced with a

permanent license. To obtain a permanent license, you must first obtain the Server's HOST ID. To view the HOST ID, click on the "Server Tab" and select "Server Administration."

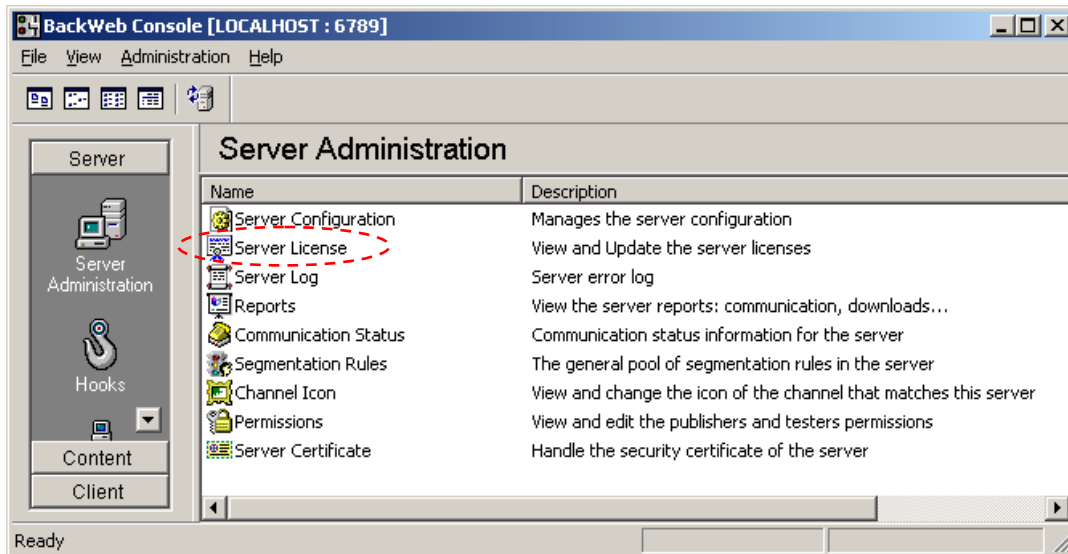


Figure 34: Server Console

In the "Server Administration" window, click on the "Server License" item (**Figure 34**).

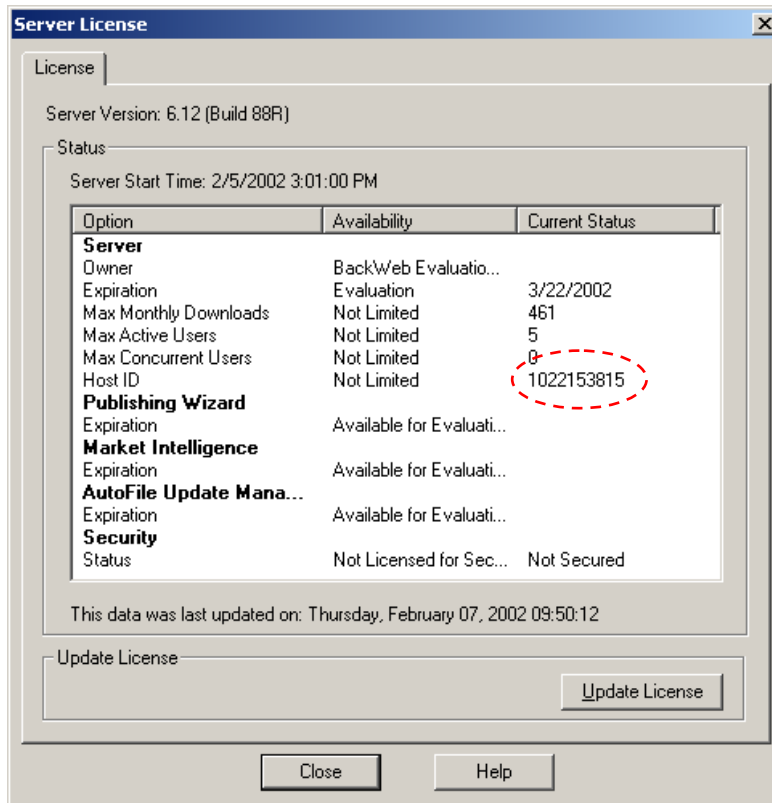


Figure 35: Server License

This will bring up the Server License page (**Figure 35**). Look for the “Host ID” field and write this number down. This number must be provided to BackWeb Support and they will issue a permanent server license file and email it. To continue with the installation without the permanent license, proceed to the *Custom Package Importer (Perl Script)* section.

BackWeb Server Permanent License Installation

Once the license file is received from BackWeb, return to the BackWeb Console, open the Server License page (**Figure 35**), and click on the “Update License” button.

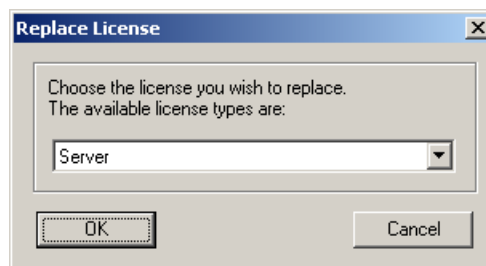


Figure 36: Replace License

The “Replace License” dialogue will be displayed (**Figure 36**). Ensure that “Server” is selected in the drop-down box and click “Ok.”

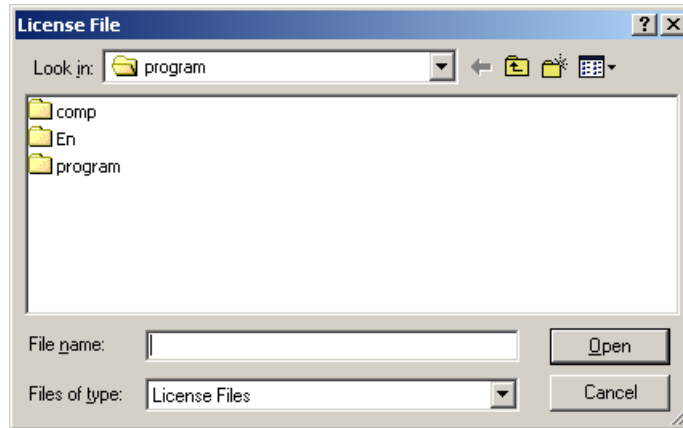


Figure 37: License File

Select the permanent license file that BackWeb support sent (**Figure 37**) and click “Open” to install it.

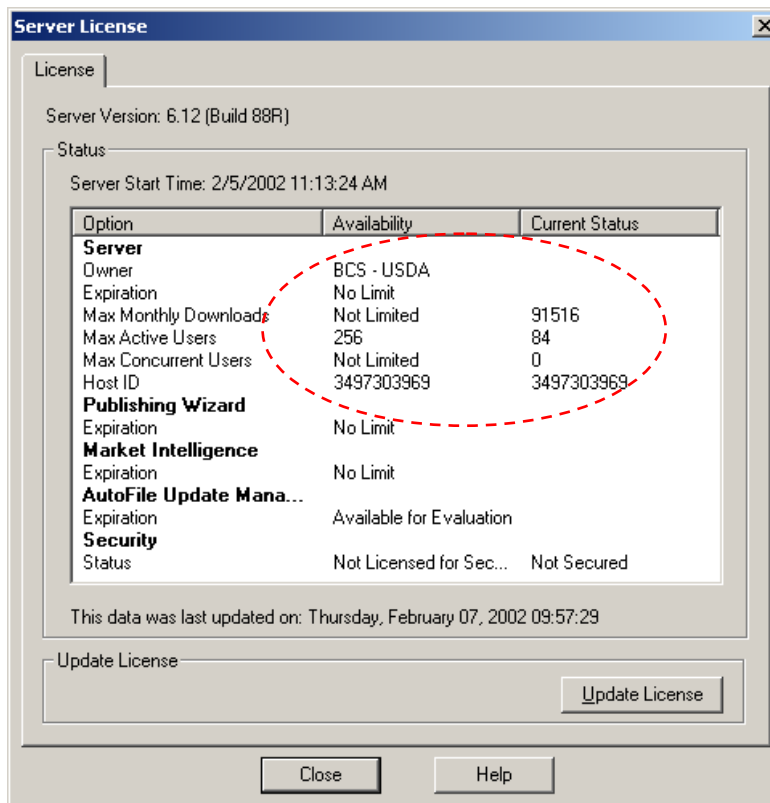


Figure 38: Updated License

The “Server License” page should now be updated with the new license information (**Figure 38**). Note that the BackWeb server will need to be restarted for the updated license to take effect.

Custom Package Importer (Perl Script)

In order for the Market News Communication System to function properly, a custom PERL script must be installed. This PERL script runs periodically (currently every minute) and scans the “mkt_news” directory looking for new content. When new reports

are found here, they are imported into BackWeb as a new INFOPAK. The PERL script requires that the following files are installed in the “Program Files\BackWeb\BackWeb Server\USDA\PROGRAMS” directory (this directory does not exist by default):

_USDA1.BIS	USDA.END	USDA1.BIF
USDA1.BII	USDA1.BIS	USDA1.PL

The USDA1.PL script may need to be modified, depending upon the location of the “mkt_news” directory. On the new BackWeb server, the “mkt_news” directory is located on the “F:” drive (which is located on the RAID5 volume). To ensure that the PERL script will run properly, open the USDA1.PL file in a text editor and look for the following line:

```
# The existing directory for USDA's text files
$USDA_TEXT='F:/mkt_news';
```

Ensure that the correct path is listed here. (Note that PERL uses the UNIX convention of forward slashes to denote directory boundaries, unlike the Windows backslash; make sure that any modifications utilize the correct syntax).

If any of the programs were installed in non-standard paths, verify that other path references (such as \$USDA_PROG) do not need to be modified as well.

Scheduling the PERL script

The PERL script installed above must be scheduled to run on a regular basis in order for new content to be imported into the BackWeb system. This is done through “Scheduled Tasks.” To schedule this task, select “*Start | Programs | Accessories | System Tools | Scheduled Tasks.*” Double click on the “Add Scheduled Task” icon and click “Next” to begin the scheduled task wizard. You will be prompted to select the program to run (**Figure 39**).

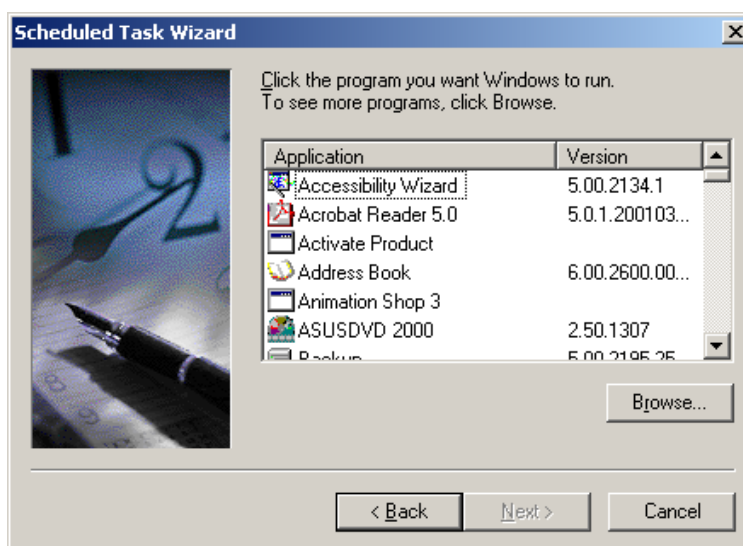


Figure 39: Scheduled Task Wizard - Select Program

Click on the “Browse” button and select the “C:\Program Files\BackWeb\BackWeb Server\USDA\PROGRAMS\USDA1.PL” file.

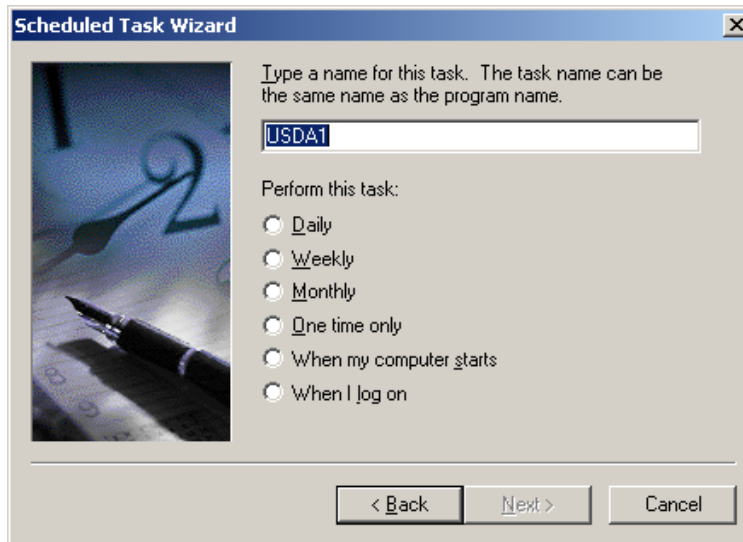


Figure 40: Scheduled Task Wizard – Name and Schedule

The wizard will now prompt for a name and schedule for the task (**Figure 40**). By default, the name will be the same as the program selected (in this case USDA1). Under “Perform this task:” select “Daily” and click “Next.”



Figure 41: Schedule Task Wizard – Date and Time

The next screen will specify the time/date for the task to run (**Figure 41**). By default it will be the current time and date. This will be modified later, so accept the default and click “Next.”



Figure 42: Scheduled Task Wizard – Credentials

The next screen will prompt for an account name and password (**Figure 42**). The local “mnscs_nt1” account and password should be entered here. When the PERL script is run, it will run under this security context. Click “Next” to continue.

Note: If the password for the “mnscs_nt1” account is changed for any reason, this scheduled task will need to be updated accordingly. This can be done at any time by selecting the properties of the Scheduled Task and clicking on the “Set Password” button.



Figure 43: Scheduled Task Wizard - Summary

The Summary page will state that the task was successfully scheduled (**Figure 43**). Check the “Open advanced properties for this task when I click Finish” box and click “Finish.”

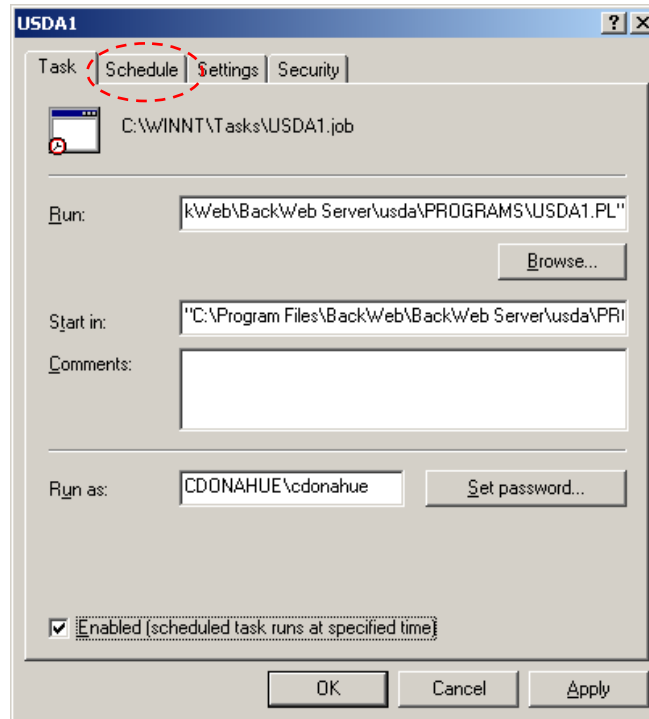


Figure 44: Scheduled Tasks – Advanced Properties

The advanced properties page for the newly scheduled task will be displayed (**Figure 44**). Click on the “Schedule” tab.

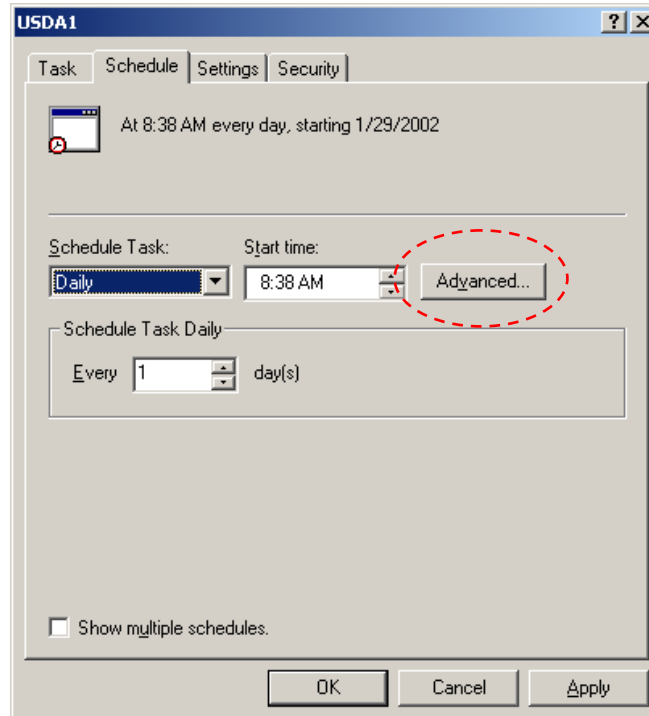


Figure 45: Schedule Tab

To configure the task to run at one minute intervals, click on the “Advanced” button (**Figure 45**).

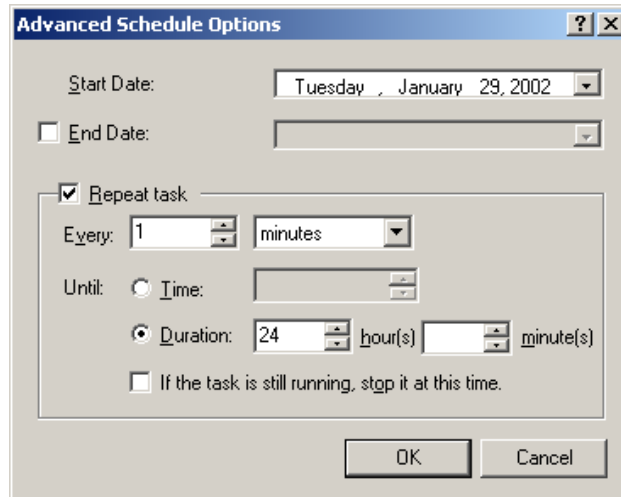


Figure 46: Advanced Schedule Options

This will bring up the “Advanced Schedule Options” dialogue box (**Figure 46**). Check the “Repeat Task” box and make the following changes:

- Change the frequency to read “Every 1 minute.”
- Click on “Duration” and configure it to read “24 hours.”

Click on “Ok” and apply the changes. This should launch the USDA1.PL script at 1 minute intervals, 24 hours a day.

Note that unlike the previous system, there will be no “DOS” box that appears periodically, and the script will run even if no one is logged onto the system. To verify that the script is running, open “Scheduled Tasks” and view the “Next Run Time” and “Last Run Time” columns (you may need to scroll to the right to see them). These columns should be updated every minute after the script has run.

CHANNEL REGISTRATION PAGE

Background

The Process of “Registering” to the USDA channel points the BackWeb Client software to the appropriate server. During the registration process, the user first connects to a web page (hosted on the BackWeb Server) which contains an HTML form (**Figure 47**).

The screenshot shows a web browser window titled "MNCS Document Delivery Registration Form - Microsoft Internet Explorer". The address bar displays "http://151.121.3.170:8080/mncs_reg.htm". The page features the USDA logo and the title "Document Delivery Registration (MNCS)". A green-bordered box contains the instruction: "To register with the Market News Communications System, please provide the following information:". Below this, there are four input fields: "Name:", "Company Name:", "Email Address:", and "Phone Number:". At the bottom of the box are "Submit" and "Reset" buttons. The browser's status bar at the bottom shows "Done" and "Internet".

Figure 47: User Registration Page

Information about the user is collected (e.g. Name, Email address). Upon submission, the information is written to an Access database stored on the BackWeb Server. (The registration page utilizes an ASP page to connect to an ODBC datasource).

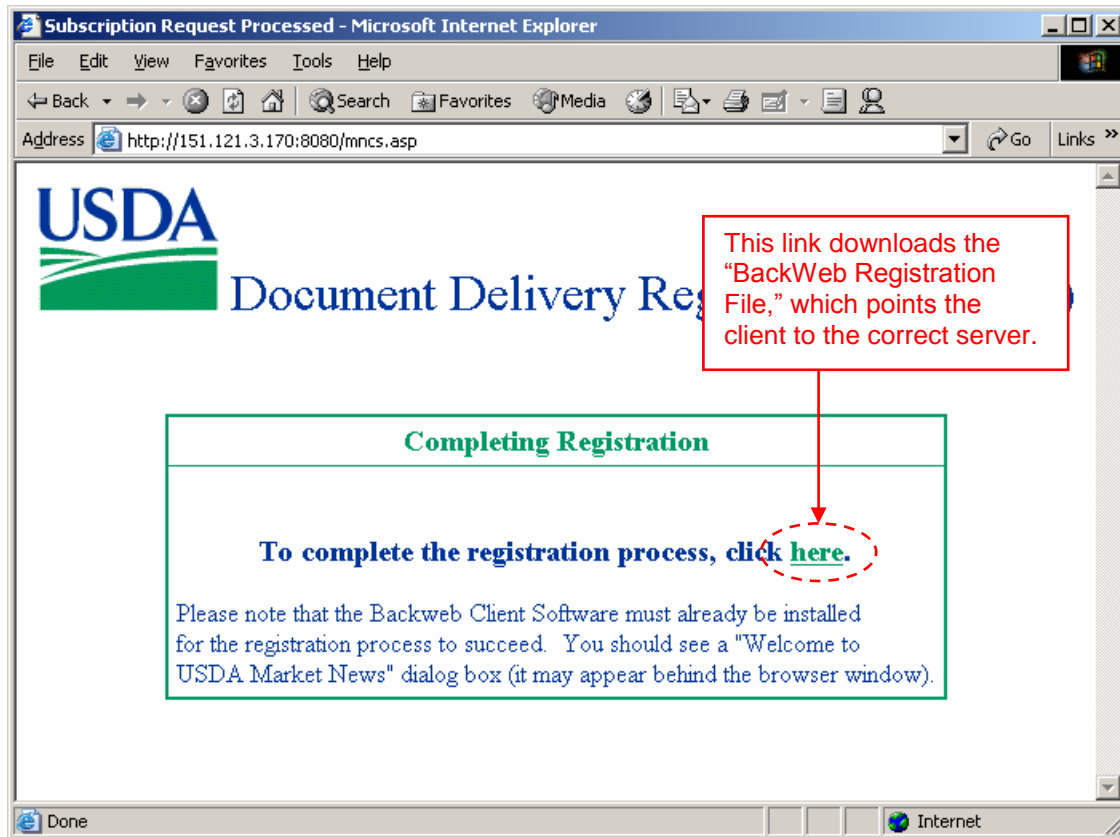


Figure 48: Completing BackWeb Registration

The user is then presented with a link to a “BackWeb Registration File” (**Figure 48**). The BackWeb Registration file contains the information necessary for the BackWeb Client to connect to the BackWeb Server. When the user clicks on the link, this will configure the necessary connection settings in their BackWeb Client.

In order to install the BackWeb registration functionality, the following steps must be performed:

1. The necessary web pages and related files must be copied to the server
2. The ODBC datasource must be configured
3. The IIS web site must be configured to return the correct MIME type for the BackWeb Resgistration File

File Installation

The following files must be installed in the root of the Default Web Site (generally C:\inetPub\wwwroot):

ARROW.GIF	BOTGRP5.GIF	BW.GIF	bwreg.bw	default.htm
DOWNLOAD.GIF	GREEN-LI.GIF	GREENBA.GIF	ICON.GIF	LOGO2.GIF
MNCS.asp	mncs reg.htm	REGISTER.GIF	RESET.GIF	SUBMIT.GIF
USDAHEAD.GIF	usdalogo.gif			

The MNCS .mdb file (the database to which user registration information is written) should be copied to the root of the C: drive. *Note that the database should **NOT** be placed*

anywhere under the `InetPub\wwwroot` directory (this would allow an Internet user to download the database).

ODBC Configuration

The `mncs.asp` page requires that an ODBC datasource named MNCS exists on the server. To create this DSN, open the ODBC Datasource Administrator application by selecting “Start | Programs | Administrative Tools | Data Sources (ODBC).”

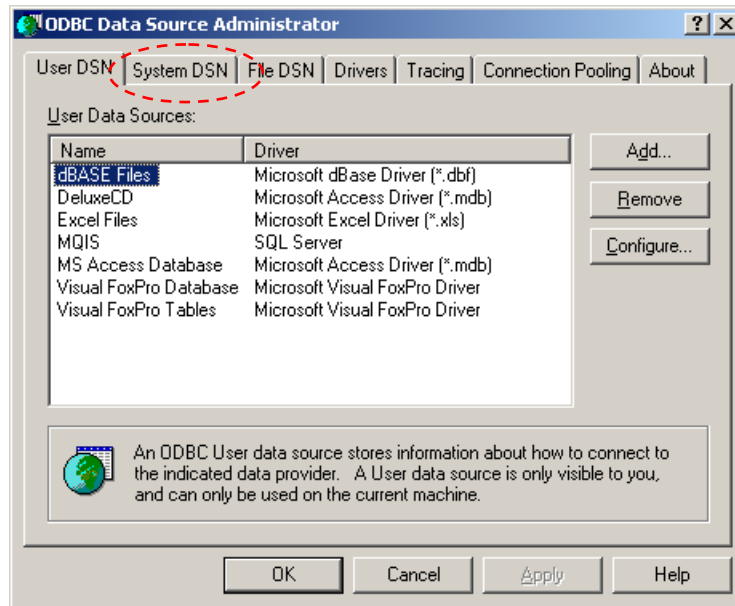


Figure 49: Data Source Administrator

Click on the “System DSN” tab (**Figure 49**) and click “Add” to create a new System DSN.

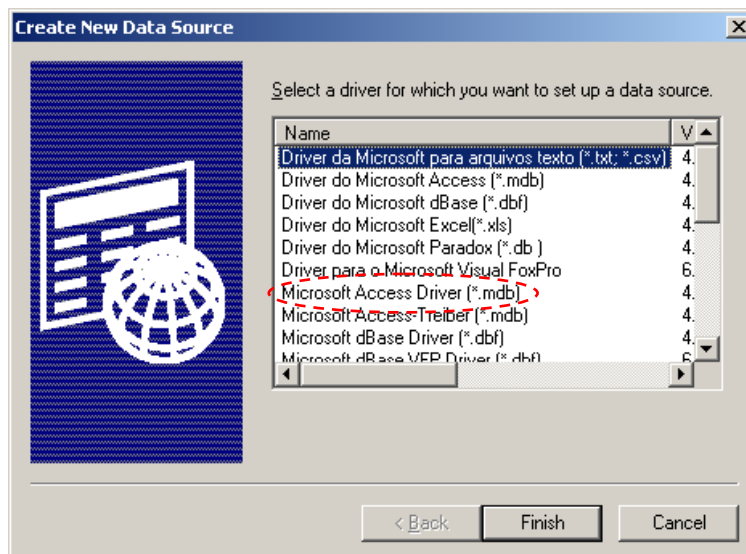


Figure 50: Create New DSN Wizard

The “Create New Data Source” Wizard will be displayed (**Figure 50**). Select the “Microsoft Access Driver (*.mdb)” and click “Finish.”

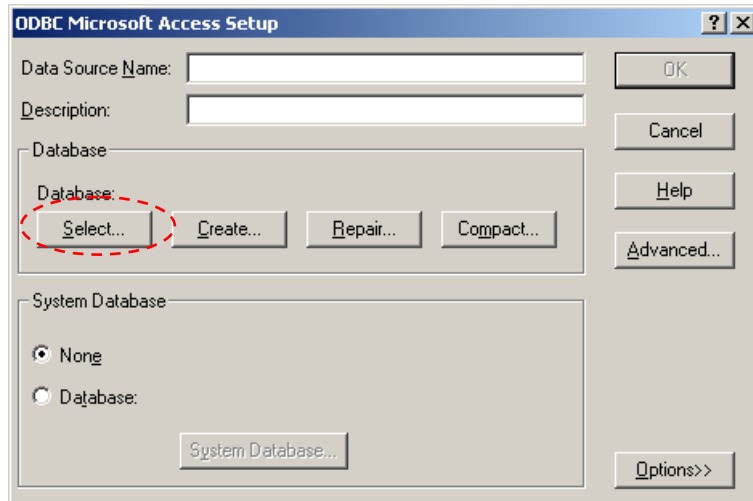


Figure 51: Data Source Properties

The properties for the newly created DSN will be displayed (**Figure 51**). Type in “**MNCS**” in the Data Source name field. Under “Database,” click on the “Select” button and select the C:\mncs.mdb file copied in the previous section. Click “OK” when finished.

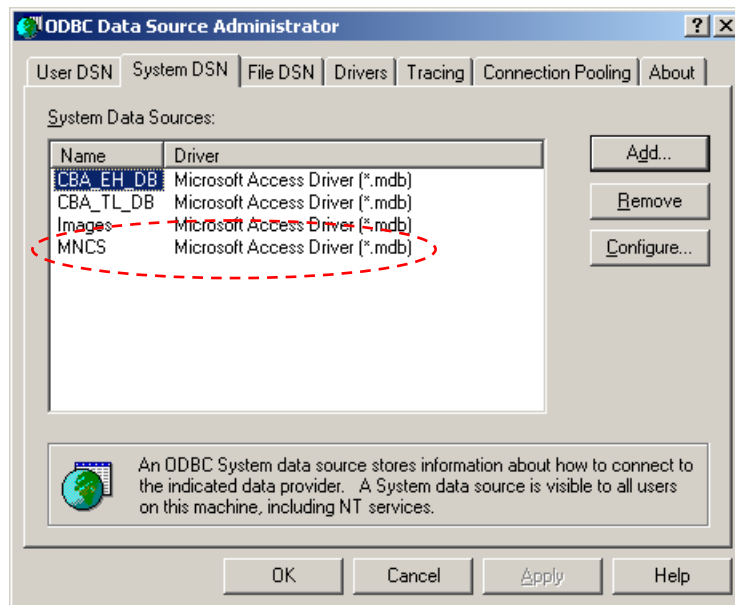


Figure 52: MNCS Data Source Created

The newly created MNCS Data Source should now appear in the listing of System DSNs (**Figure 52**). Click “OK” to accept the changes and exit out of the ODBC Datasource Administrator.

MIME Type Configuration

In order for the BackWeb registration to operate correctly through the web site, IIS must be configured to return the proper MIME header for backweb registration files. To do this, open the Internet Services Manager and select the properties of the Default Web Site.

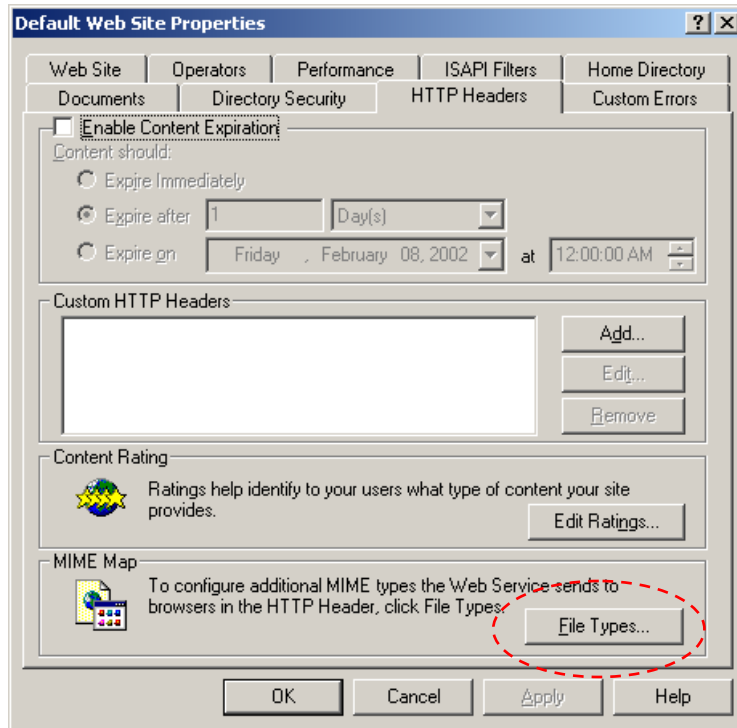


Figure 53: HTTP Headers Page

Select the “HTTP Headers” tab, and under the section for “MIME Map,” click on the “File Types” button (**Figure 53**). In the “File Types” dialogue, click on “New Type” to create a new MIME mapping.

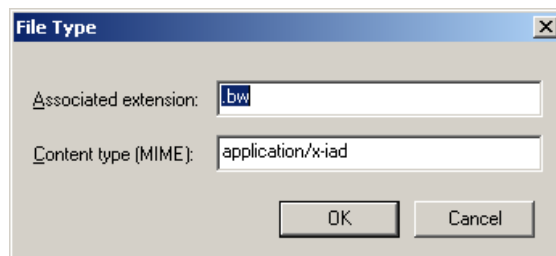


Figure 54: New File Type

The “File Type” window will appear (**Figure 54**). Type “.bw” in the “Associated Extension” box and “application/x-iaa” in the “Content Type (MIME)” box. Click “Ok” to finish.

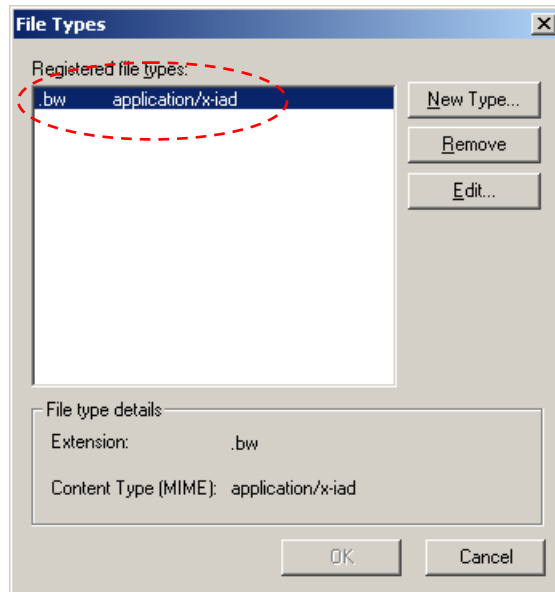


Figure 55: File Type Added

The new MIME mapping should now be listed in the “File Types” dialogue box (**Figure 55**). Click on “Ok” to save the changes to the MIME Map and close the Web Site Properties.

BACKWEB FAILOVER

Market News utilizes multiple BackWeb Servers in order to ensure availability of the service should one of the BackWeb servers fail. The current failover model utilizes two servers, both located in the USDA South Building (Washington, DC). Although both servers are powered on at all times, BackWeb clients only connect to the primary server (151.121.3.170, which is translated to 10.10.1.1 at the firewall). In the event of a failure of the primary BackWeb Server, the following procedures can be followed to bring the backup server online as the primary:

1. The primary BackWeb Server is brought offline (e.g. powered down and/or unplugged from the network).
2. The IP address on the Backup BackWeb server (10.10.1.14) is changed to the IP address formerly used by the Primary BackWeb server (10.10.1.1).
3. In the BackWeb Console, any InfoPaks on the server prior to the current day's are deleted.

Client connections will now be made to the Backup BackWeb server. The same process can be repeated to bring the Primary BackWeb Server back online.

APPENDIX A: INSTALLATION CHECKLIST

1. Installed Windows 2000 ☐
 - a. Configured RAID/created partitions (if necessary) ☐
 - b. Installed correct Windows 2000 Components ☐
 - c. Installed Windows 2000 SP2 ☐
 - d. Installed Installed Hotfixes (Security Rollup) ☐
 - e. Installed as a stand-alone server ☐
 - f. Created mncs_nt1 local account ☐
 - g. Created mkt_news and mkt_news2 directories ☐
 - h. Set security and shared mkt_news directories ☐
2. Configured IIS ☐
 - a. Changed Default Web Site port to 8080 ☐
 - b. Removed unnecessary directories and virtual directories ☐
 - c. Removed unnecessary ISAPI mappings ☐
 - d. Disabled Web Based Printing ☐
3. Installed Additional Software ☐
 - a. Installed BackWeb Server ☐
 - b. Installed BackWeb Console ☐
 - c. Installed BackWeb Automation SDK/PERL ☐
4. Configured BackWeb ☐
 - a. Added USDA Sub-Channel ☐

- b. Added Satellite Exposure Group ☐
 - c. Acquired and installed BackWeb Server License ☐
- 5. Installed Custom Package Importer (PERL script) ☐
 - a. Copied required files to server ☐
 - b. Modified PEL script to point to the correct path ☐
 - c. Scheduled PERL script to run through Scheduled Tasks ☐
- 6. Installed Channel Registration Pages ☐
 - a. Copied required files to wwwroot ☐
 - b. Created ODBC Datasource ☐
 - c. Configured MIME type in IIS ☐
- 7. Brought Server Online and Tested Functionality ☐

VERSION CONTROL

<i>Date</i>	<i>Version</i>	<i>Author(s)</i>	<i>Summary of Changes</i>
2/8/2002	1.0	Chris Donahue	Initial Document